Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

Пояснювальна записка

до магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:
ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ
08-34.МКР.001.00.000 ПЗ

Виконала: студент 2-го курсу,
групи ТКС-18м
спеціальності 172 – Телекомунікації та радіотехніка _____.

_____ Бакіссі Едена Маурісіна Бонже

Керівник: к.т.н., доцент каф. ТКСТБ

_____ Стальченко О.В.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф. РТ

_____ Гаврілов Д.В.

«____» _____ 2019 р.

Вінниця ВНТУ - 2019 рік

Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення
Освітньо-кваліфікаційний рівень магістр
Галузь знань 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ТКСТБ
к.т.н., професор Г.Г. Бортник

“___” _____2019 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Бакіссі Едена Маурісіна Бонже .
(прізвище, ім’я, по батькові)

1. Тема роботи Підвищення інформаційної безпеки IP-телефонії

керівник роботи Стальченко Олександр Володимирович, канд. техн. наук, доцент,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “02” 10 2019 року № 254
2. Строк подання студентом роботи 02 грудня 2019 року

3. Вихідні дані до роботи 1. Клас якості обслуговування - 0; 2. Затримка доставки пакета IP, IPTD – 100 мс; 3. Варіація затримки пакета IP, IPDV (джиттер) – 50 мс; 4. Коефіцієнт втрати пакетів IP, IPLR - 10^{-3}; 5. Коефіцієнт помилок пакетів IP, IPER - 10^{-4}; 6. Протокол захисту при встановленні з’єднання - SIPS / TLS; 7. Протокол захисту при передаванні медіа-трафіку – SRTP; 8. Протокол захисту при розділенні ключів - ZRTP, SDES; 9. Метод підтримки VPN – PPTP.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Аналіз поточного стану справ в області захищеної IP-телефонії; 2. Математична модель активного несанкціонованого доступу для захищеної IP-телефонії; 3. Розробка пропозицій щодо вдосконалення протоколів розподілу ключів; 4. Розробка пропозицій щодо поліпшення ймовірнісно-часових характеристик протоколу ZRTP.
5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)
1. Принципова схема підключення оператора VoIP; 2. Архітектурна модель для підтримки QoS; 3. Структурна схема з'єднання в сценарії клієнт-клієнт; 4. Алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником; 5. Алгоритм дій при захопленні терміналу користувача зовнішнім порушником; 6. Алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником; 7. Алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Стальченко О.В., доцент кафедри ТКСТБ		
Економічна частина	Кавецький В.В., старший викладач		
Охорона праці та безпека в надзвичайних ситуаціях	Березюк О.В. к.т.н., доцент		

7. Дата видачі завдання 02 вересня 2019 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	06.09.2019р.	
2.	Аналіз поточного стану справ в області захищеної IP-телефонії	13.09.2019р.	
3.	Математична модель активного несанкціонованого доступу для захищеної IP-телефонії	04.10.2019р.	
4.	Розробка пропозицій щодо вдосконалення протоколів розподілу ключів	25.10.2019р.	
5.	Розробка пропозицій щодо поліпшення ймовірнісно-часових характеристик протоколу ZRTP	08.11.2019р.	
6.	Аналіз економічної ефективності розробки	15.11.2019р.	
7.	Охорона праці та безпека в надзвичайних ситуаціях	22.11.2019р.	
8.	Оформлення пояснювальної записки та графічної частини	29.11.2019р.	
9.	Нормоконтроль МКР	02.12.2019р.	
10.	Попередній захист МКР, рецензування МКР	06.12. 2019р.	
11.	Захист МКР ЕК	09.12. 2019р.	

Студент _____ Бакіссі Едена Маурісіна Бонже
(підпис)

Керівник роботи _____ Стальченко О.В.
(підпис)

РЕФЕРАТ

УДК 621.391

Бакіссі Едена Маурісіна Бонже. Підвищення інформаційної безпеки IP-телефонії. Магістерська кваліфікаційна робота зі спеціальності «Телекомунікації та радіотехніка» – Вінниця: ВНТУ, 2019. – 109 с. На українській мові.

Рисунків 46, таблиць 13, бібліографія 41.

Розглянуто модель порушника, яка враховує атаку на протоколи забезпечення безпеки IP- телефонії.

Здійснено оцінювання ймовірнісно-часових характеристик протоколів розподілу ключів, які зумовлюють обмеження числа повторних передач повідомлень зі змінним таймером повторної передачі при роботі по каналах з помилками і затримками.

Розглянуто метод виявлення порушника протоколів у використовуваних каналах зв'язку при відсутності загального довіреного центру або ключа між кореспондентами, а також автоматичного виявлення порушника, що володіє технологією синтезу голосу.

Досліджено модифікований протокол з зменшеними часовими витратами при роботі у каналах зв'язку із затримками та помилками.

ABSTRACT

UDC 621.391

Baquisse Edena Mauricina Bonge. Improving information security of IP-telephony. Master's qualification work in the specialty "Telecommunications and Radio Engineering" - Vinnytsia: VNTU, 2019. - 109 p. In Ukrainian language.

Figures 46, tables 13, bibliography 41.

The model of the intruder considering the attack on IP telephony security protocols is considered.

The probabilistic-temporal characteristics of the key-allocation protocols are estimated, which cause a restriction on the number of retransmissions of messages with a variable retransmission timer when working on channels with errors and delays.

The method of detection of the protocol violator in the used communication channels in the absence of a common trust center or key between correspondents, as well as the automatic detection of the intruder with the technology of voice synthesis is considered.

A modified protocol with reduced time costs when working in delay and error communication channels was investigated.

ЗМІСТ

ВСТУП 6
1 АНАЛІЗ ПОТОЧНОГО СТАНУ СПРАВ В ОБЛАСТІ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ 10
1.1 Принципи передачі голосової інформації в мережах з пакетною комутацією 10
1.1.1 Класифікація протоколів IP-телефонії 10
1.1.2 Сценарії встановлення з'єднання в IP-телефонії 12
1.2 Забезпечення якості в IP-телефонії 14
1.2.1 Показники якості IP-телефонії 14
1.2.2 Методи забезпечення якості в VoIP 16
1.2.3 Методи оцінки якості VoIP і стан досліджень 19
1.3 Забезпечення інформаційної безпеки IP- телефонії 23
1.3.1 Протоколи забезпечення безпеки IP-телефонії 24
1.3.2 Протоколи генерації і розподілу ключів для захисту медіаінформації 25
1.3.3 Вимоги до протоколів розподілу ключів 28
1.3.4 Стан досліджень щодо захисту голосових зв'язків при використанні IP-телефонії 29
1.4 Постановка наукових завдань дослідження МКР 30
1.5 Висновки до розділу 1 32
2 МАТЕМАТИЧНА МОДЕЛЬ АКТИВНОГО ПОРУШНИКА ДЛЯ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ 34
2.1 Загрози інформаційної безпеки в IP-телефонії 35
2.2 Узагальнена модель порушника 36
2.3 Приватні моделі порушників 40
2.3.1 Зовнішній порушник 41
2.3.2 Внутрішній порушник 49
2.4 Оцінка ймовірності успішного завершення атаки 53
2.5 Висновки до розділу 2 56
3 РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ВДОСКОНАЛЕННЯ ПРОТОКОЛІВ РОЗПОДІЛУ КЛЮЧІВ 58
3.1 Метод підвищення безпеки ZRTP за рахунок автоматичної перевірки аутентифікаційного рядка 60

3.2 Метод виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі- Хелмана 66
3.2.1 Оцінки ймовірностей результатів розподілу ключів при використанні декількох каналів зв'язку 66
3.3 Висновки до розділу 3 74
4 РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПОЛІПШЕННЯ ЙМОВІРНОСНО-ЧАСОВИХ ХАРАКТЕРИСТИК ПРОТОКОЛУ ZRTP 76
4.1 Висновки до розділу 4 83
5 ЕКОНОМІЧНА ЧАСТИНА 85
5.1 Розрахунок витрат на проведення НДДКР з дослідження підвищення інформаційної безпеки IP-телефонії 85
5.2 Визначення коефіцієнта наукової значимості отриманих результатів науково-дослідної роботи 90
5.3 Внесок дослідника в досягнення отриманих результатів НДР 92
5.4 Висновки до розділу 5 92
6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 93
6.1 Гігієна праці та виробнича санітарія 93
6.1.1 Склад повітря робочої зони та мікроклімат 93
6.1.2 Виробниче освітлення 94
6.1.3 Виробничі віброакустичні коливання 95
6.1.4 Виробничі випромінювання 96
6.2 Технічні рішення з промислової та пожежної безпеки при проведенні удосконалення інформаційної безпеки IP-телефонії 97
6.2.1 Безпека щодо організації робочих місць 97
6.2.2 Електробезпека 97
6.2.3 Пожежна безпека 97
6.3 Безпека в надзвичайних ситуаціях 98
6.3.1 Визначення області працездатності мережі IP-телефонії в умовах дії загрозливих чинників надзвичайних ситуацій 98
6.3.2 Визначення області працездатності мережі IP-телефонії в умовах дії іонізуючих випромінювань 99
6.3.3 Визначення області працездатності мережі IP-телефонії в умовах дії електромагнітного імпульсу 100
6.3.4 Розробка заходів по підвищенню безпеки роботи мережі IP-телефонії в умовах дії електромагнітного імпульсу 101

6.4 Висновки до розділу 6 101
ВИСНОВОК 102
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 103
ДОДАТКИ 110
Додаток А (Технічне завдання) 111
Додаток Б (Принципова схема підключення оператора VoIP) 112
Додаток В (Архітектурна модель для підтримки QoS) 113
Додаток Г (Структурна схема з'єднання в сценарії клієнт-клієнт) 114
Додаток Д (Алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником) 115
Додаток Е (Алгоритм дій при захопленні терміналу користувача зовнішнім порушником) 116
Додаток Є (Алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником) 117
Додаток Ж (Алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником) 118

ВСТУП

Актуальність теми дослідження. Сучасному періоду розвитку телекомунікацій відповідають зростаючі обсяги трафіку в корпоративних мережах, зокрема, в мережах Інтернет провайдерів.

IP-телефонією називають технологію передачі мови по мережах з пакетною комутацією на базі протоколу IP [1]. Як правило, під цим визначенням також мають на увазі набір протоколів, методів і технологій, що забезпечують голосове спілкування через мережу з комутацією пакетів. Причинами поширення IP-телефонії послужили низька вартість в порівнянні з аналоговою телефонією, викликана застосуванням недорогих мереж з комутацією пакетів, а також універсальність і мобільність, що дозволяє перетворити мова в потік даних в будь-якій точці мережевий інфраструктури.

Розвиток нових протоколів, а також передача голосових пакетів у відкритому вигляді через публічні мережі привели до появи і стандартизації протоколів забезпечення безпеки IP-телефонії. Протоколи були розділені на три групи в залежності від розв'язуваних задач: забезпечення безпеки сигналізації, захист медіа трафіку і розподіл ключів для медіа трафіку.

Стандартизація протоколів, а також поширене використання персональних комп'ютерів в якості терміналів користувача для послуг IP-телефонії привели до розробці широкого кола програм для IP-телефонії, в тому числі програмного забезпечення (ПО) з відкритим вихідним кодом, що дозволяє розширювати можливості і використовувати додаткові алгоритми в програмах.

Таким чином, магістерська кваліфікаційна робота, присвячена дослідженню протоколів забезпечення інформаційної безпеки IP-телефонії, а також розробці пропозицій щодо вдосконалення цих протоколів для підвищення безпеки і ефективного функціонування при роботі по каналах зв'язку з різними параметрами, відповідає сучасній науковій проблематиці і є актуальною.

Ступінь розробленості теми. Проводяться наукові дослідження в областях забезпечення безпечної передачі інформації, забезпечення якості при передачі голосових і мультимедійних файлів, стиснення мови і відео, оцінки якості надання послуг IP- телефонії. Дослідження в області забезпечення безпеки даних в IP- телефонії приведені в роботах Нопіна С.В., Майстренко В. А, Шахова В.Г [2- 4], Гомін Т.А. [5], Докучаєва В.А., Шведова А.В [6], Макарової О.С. [7], Крюкова Ю.С. [8] та ін .; дослідження протоколів забезпечення безпеки IP- телефонії - в роботах Оніка Е. [9], Riccardo Bresciani і Andrew Butterfield, Charles V Wright, Vitaly Shmatikov, Prateek Gupta [10] та

ін .; дослідження в області атак MITM і методів захисту від них описуються в роботах Атрощенко В.А., Руденко М.В., Липатникова В.А, Дьяченко Р.А., та ін. [11]; дослідження методів забезпечення безпеки протоколів - в роботах Ф. Циммермана, Дем'янчука А.А., Новикова Е.С., Молдовяна А.А, Молдовяна Д.Н ,; забезпечення QoS (Quality of Service) і оцінка якості, а також моделювання мереж IP-телефонії - в дослідженнях Krzysztof Perlicki, Сухова А. М., Мошака М.М., Рудинской С.Р., Федосеевой О. С. [8], Erol Gelenbe, Ricardo Lent, Rafik A. Goubran, P.Eng. та ін. Значний внесок в дослідження тимчасових характеристик внесли Нікітін В.М., а також Нсангу М. М., Юркін Д. В., Вінель А. В., Таранін В. В., Галкін А.М., Яновський Г.Г., Петрова М.Н., Лосєв Ю.І., Руккас К.М..

Однак залишається недостатньо освітленим питання забезпечення безпеки для сценарію IP-телефонії точка-точка в разі, коли кореспонденти не мають заздалегідь виробленого ключового матеріалу. Також залишаються маловивченими ймовірносно-часові характеристики протоколів безпеки IP-телефонії і питання про вплив цих протоколів на виконання встановлених норм при використанні IP-телефонії.

У роботах Нопіна С.В. [3], Макарової О. С., Докучаєва В.А. , Миронова В.Г. наводяться описи моделей порушника безпеки інформаційних систем, в тому числі порушника в IP-телефонії. Однак загальним недоліком робіт є те, що не описується атака "Людина посередині" на протоколи розподілу ключів. Таким чином доцільно розробити нову модель порушника, що враховує цю атаку.

Об'єктом дослідження є захищена IP-телефонія, а предметом дослідження - методи і протоколи забезпечення інформаційної безпеки IP-телефонії, а також ймовірносно-часові характеристики цих протоколів.

Мета і завдання дослідження. Метою є підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії і скорочення часу встановлення захищеного з'єднання. Для досягнення поставленої мети вирішені наступні завдання:

- дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості;
- розробка моделі порушника для оцінки захищеності системи IP-телефонії;
- розробка методики оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії;
- розробка пропозицій щодо модифікації протоколу розподілу ключів для поліпшення ймовірносно-часових характеристик протоколу;

- розробка методу виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана;

- розробка пропозицій щодо модифікації протоколу Zimmermann Real-time Transport Protocol (ZRTP) для забезпечення безпеки кореспондентів при взаємодії без сервера в топології клієнт-клієнт.

Наукова новизна

1. Розроблена модель порушника відрізняється від відомих аналогів урахуванням атаки "людина посередині" на протоколи забезпечення безпеки IP- телефонії.

2. Методика оцінки ймовірнісно-часових характеристик протоколів розподілу ключів на відміну від існуючих враховує особливості протоколів розподілу ключів, виражені в наявності обмеження числа повторних передач повідомлень зі змінним таймером повторної передачі при роботі по каналах з помилками і затримками.

3. Метод виявлення порушника на відміну від існуючих методів дозволяє виявити активного порушника протоколів в використовуваних каналах зв'язку при відсутності загального довіреної центру або ключа між кореспондентами, а також автоматично виявити порушника, що володіє технологією синтезу голосу.

4. Модифікований протокол ZRTP, що відрізняється меншим часом успішного завершення, що знижує тимчасові витрати при роботі протоколу по каналах зв'язку з затримками і помилками.

Теоретична і практична значущість роботи. Теоретична значимість: Модель дозволяє отримати аналітичну залежність ймовірності НСД від ймовірностей проміжних атак.

Метод виявлення порушника протоколів доповнює і розвиває теорію інформаційної безпеки, в частині властивостей протоколів спільного вироблення загального ключа, а саме: пов'язує число одночасно використовуваних каналів зв'язку і стійкість протоколів захищеної IP-телефонії до атаки активного порушника.

Методика оцінки ймовірнісно-часових характеристик дозволяє розрахувати ймовірність і середній час успішного виконання протоколів розподілу ключів при роботі по каналах зв'язку з різними значеннями затримки і ймовірності помилки.

Практична значимість: Модель порушника може бути використана при розробці методик контролю захищених мереж електрозв'язку, а також в навчальному процесі з дисципліни "Безпека IP-телефонії".

Метод виявлення порушника дозволяє автоматично виявити втручання

порушника протоколів в канал зв'язку між кореспондентами для протоколу ZRTP без участі користувача. Метод дозволяє знизити ймовірність успішної атаки НСД для порушника протоколів і може бути використаний при проектуванні, розробці та реалізації рішень захищеної IP-телефонії, що мають режим роботи без сервера, а також для удосконалення існуючих рішень

Методика може бути використана для оцінки ефективності протоколів розподілу ключів, в частини часу виконання і ймовірності успішного завершення.

Методика оцінки ймовірнісно-часових характеристик може застосовуватися в розрахунках при проектуванні рішень по захищеної IP-телефонії, що використовують в своєму складі протоколи розподілу ключів.

Методологія і методи дослідження. Для вирішення поставлених завдань використовувалися методи імовірнісних графів, теорії ймовірності, комбінаторики. Для аналізу даних розроблялися додаткові прикладні програми з використанням об'єктно-орієнтованого програмування. Для експериментальної оцінки використовувалося додаткове програмне забезпечення – аналізатор трафіку, Zfone і програмно-апаратний маршрутизатор на базі платформи FreeBSD для емуляції каналу зв'язку (КС).

1 АНАЛІЗ ПОТОЧНОГО СТАНУ СПРАВ В ОБЛАСТІ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ

1.1 Принципи передачі голосової інформації в мережах з пакетною комутацією

1.1.1 Класифікація протоколів IP-телефонії

Протоколи IP-телефонії поділяються на дві великі групи, а саме протоколи передачі медіа інформації по пакетним мереж, а також протоколи управління встановленням з'єднання.

В першу групу входить протокол RTP (Real-time Transport Protocol) [17], що працює поверх UDP (User Datagram Protocol) протоколу. Сукупність протоколів RTP / UDP / IP забезпечує транспортний механізм для мовного трафіку.

Протоколи другої групи забезпечують управління при обслуговуванні виклику між абонентами.

До цієї групи належать протоколи SIP (Session Initiation Protocol) [18], H.323, MGCP (Media Gateway Control Protocol) [19]. Протоколи встановлення з'єднання можуть працювати як поверх UDP транспорту, так і по TCP (Transmission Control Protocol). Таким чином, сукупність протоколів (SIP / H.323 / MGCP) / (UDP / TCP) / IP формують сигнальний механізм для передачі мовного і медіа трафіку.

Історично першим протоколом для IP-телефонії, який отримав широке поширення, став H.323, представлений Міжнародним союзом електрозв'язку в рекомендації H.323. Документ описує кілька протоколів, які спільно забезпечують роботу мультимедійних протоколів в мережах з негарантованих якістю обслуговування. Однак, H.323 має досить складну структуру, так як протокол спочатку розроблявся для інтеграції телефонної мережі загального користування (ТМЗК) з мережами передачі даних.

Управління викликами може бути реалізовано за рахунок використання протоколу MGCP, архітектура якого складається з декількох елементів:

1) Шлюз - Media Gateway, що виконує функції перетворення мовної інформації з ТМЗК в мережу з комутацією пакетів;

2) Контролер шлюзів - Call Agent, керуючий шлюзами;

3) Шлюз сигналізації - Signaling Gateway (SG), що забезпечує передачу сигналізації, що надходить з ТМЗК, до контролера шлюзів і в зворотному напрямку.

Особливостями MGCP є зосередження всього інтелекту розподіленого шлюзу в контролері і можливість розділення функцій контролера між декількома обчислювальними платформами.

Третім протоколом, що дозволяє здійснювати управління викликами, є SIP [40]. SIP базується на протоколі HTTP, має більш просту структуру в порівнянні з H.323 і MGCP. Завдання протоколу - зробити абонентські пристрої і шлюзи більш інтелектуальними, а також забезпечити розширюваність протоколу для підтримки додаткових послуг для користувачів. Підхід до побудови мереж IP-телефонії на базі протоколу SIP набагато простіше, ніж реалізація на H.323 і MGCP. З цієї причини - SIP протокол отримав широке розповсюдження. Так, наприклад, оператор Ростелеком, що займає одне з перших місць на ринку надання послуг телефонного зв'язку в Росії - переводить абонентів на VoIP з оновленням мережі на GPON, використовуючи при цьому SIP протокол на мережі і абонентські пристрої GPONONT.

Крім наведеної вище класифікації протоколів IP-телефонії, можна додатково виділити кілька підсистем, що функціонують для надання послуг VoIP [1]:

• Підсистема забезпечення якості;
• Підсистема забезпечення безпеки IP-телефонії;
• Підсистема білінгу і менеджменту IP- телефонії;
• Підсистема додаткових послуг;
• Підсистема забезпечення управлінням викликами і адресацією.

Підсистема забезпечення якості відповідає за підтримку якості телефонного зв'язку і включає в себе сукупність протоколів, алгоритмів і механізмів, що працюють для досягнення цієї мети.

Підсистема безпеки IP-телефонії відповідає за конфіденційність телефонних переговорів кореспондентів, а так же переданої інформації. Дана система включає в себе сукупність протоколів, механізмів і алгоритмів для забезпечення безпеки в мережі IP-телефонії.

Підсистема білінгу і менеджменту застосовується для обліку викликів користувачів, тарифікації дзвінків і виконання взаєморозрахунків між користувачами (абонентами) і оператором, що надає послугу.

Підсистема додаткових послуг відповідає за надання додаткових сервісів абонентам мережі IP-телефонії. До них відносяться: забезпечення роумінгу і мобільності, надання додаткових сервісів, таких як відео виклики, інформаційні сервіси і т.д. підсистема складається з протоколів, що застосовуються для надання додаткових послуг.

Підсистема управління викликами і адресації відповідає за виконання базових послуг VoIP, а саме:

• організація викликів і маршрутизацію викликів;

• передача голосового трафіку.

1.1.2 Сценарії встановлення з'єднання в IP-телефонії

При описі системи IP-телефонії слід окремо виділити можливі сценарії взаємодії кореспондентів. У загальному випадку сценарієм називається сукупність елементів, взаємодіючих при обробці дзвінка. У більш широкому сенсі, сценарієм може бути названа сукупність застосовуваних при обробці дзвінка протоколів, алгоритмів, механізмів, а також процедур їх взаємодії між собою для досягнення кінцевої мети.

При складанні прикладу сценарію введено допущення, що в якості протоколу сигналізації на мережі IP-телефонії застосовується протокол SIP. При складанні схеми взаємодії враховано, що згідно із законом про зв'язок, заборонено приєднання операторів один до одного за допомогою VoIP. З'єднання різних VoIP операторів дозволяється виконувати тільки через мережу ТМЗК [12].

На рис. 1.1 представлена "Принципова схема підключення оператора VoIP". На її прикладі розглянуті можливі варіанти сценаріїв обробки викликів елементами мережі IP-телефонії: користувачами (абонентами), IP-телефонними станціями (IP АТС, SoftSwitch), прикордонними шлюзами E1. Для прикладу - наведено два постачальника послуг IP-телефонії, а також оператор традиційної телефонії.

Оператор 1 надає VoIP сервіси абонентам, підключеним на мережі

1. Оператор 1 може використовувати кілька IP АТС, позначених SSx на малюнку, де x - порядковий номер IP АТС. Як правило, ймовірність виклику від абонента А1 іншому абоненту мережі того ж самого оператора (Б1 або В1) вкрай мала для невеликих і середніх компаній. Найбільш поширені дзвінки абонентам, підключеним до інших операторів.

Можливі такі сценарії з'єднання:

• А1-SS1-GW1-ТфОП-GW2-SS2-В2 (VoIP абонент однієї компанії через ТфОП дзвонить VoIP абоненту іншого оператора)

• А1-SS1-GW1-ТфОП-Г (VoIP абонент однієї компанії через ТфОП дзвонить абоненту мережі ТМЗК іншого оператора).

• А1-SS1-SS2-В1 (VoIP абонент одного оператора дзвонить іншому абоненту цього ж оператора, підключеному до додаткової IP АТС оператора)

• А1-SS1-Б1 (VoIP абонент одного оператора дзвонить іншому абоненту цього ж оператора, при цьому абоненти підключені до однієї IP АТС)

• А2-Б2 (VoIP абонент одного оператора дзвонить іншому абоненту, при це виклик здійснюється безпосередньо між кореспондентами, минаючи IP АТС).

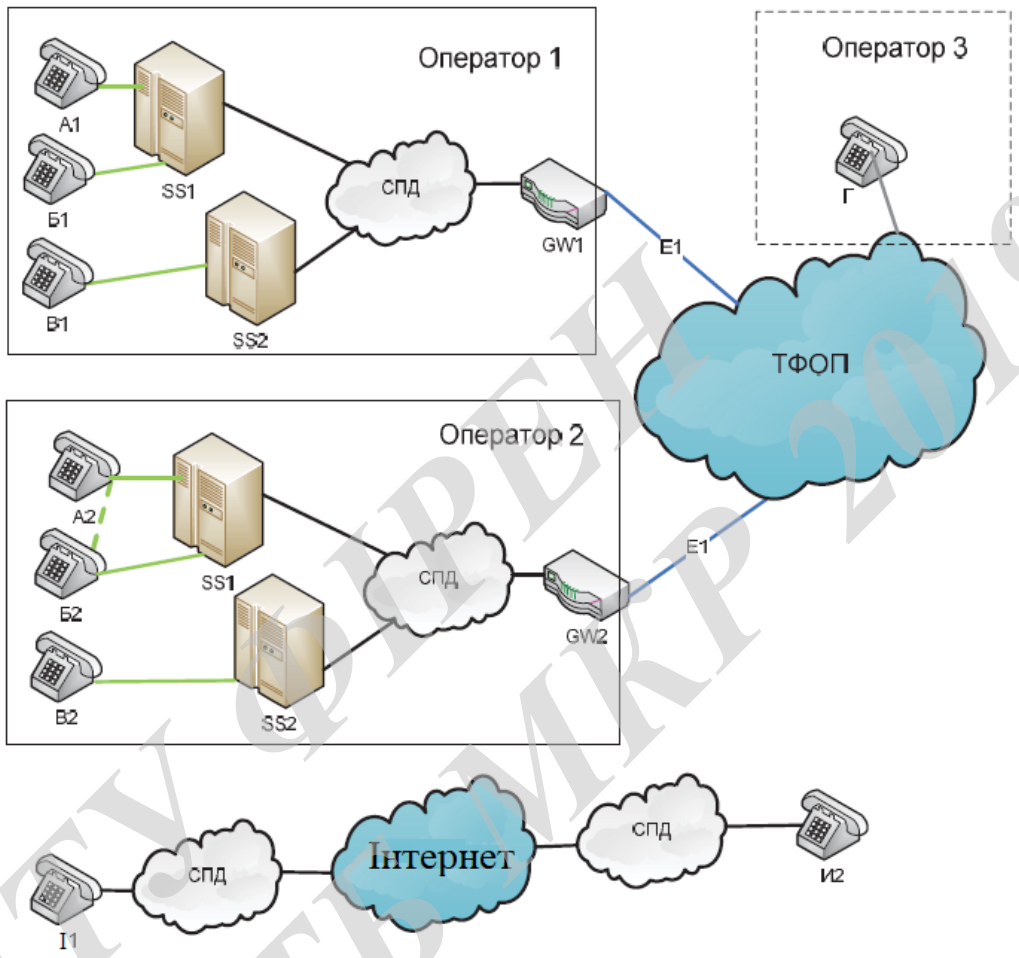


Рисунок 1.1 - Принципова схема підключення оператора VoIP

Такий спосіб найчастіше використовується, коли необхідно організувати передачу абонентської лінії традиційної телефонії по мережах IP. Спосіб з'єднатися без АТС може застосовуватися в корпоративних мережах для організації внутрішнього службового зв'язку, а також між окремими кореспондентами глобальної мережі, що не мають підключення до однієї АТС, але мають потребу проведення сеансів телефонного зв'язку в захищеному режимі.

Описані сценарії наведені також на рис. 1.2

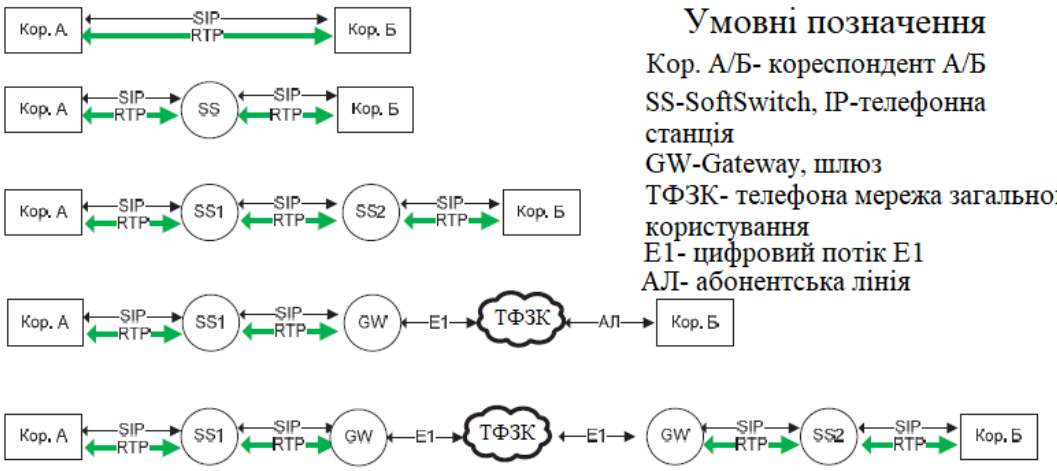


Рисунок 1.2 - Можливі сценарії встановлення з'єднання кореспондента VoIP

У всіх вищенаведених сценаріїв при обробці викликів повинні виконуватися норми, визначені для телефонного зв'язку. Однак, в сценаріях можуть застосовуватися різні протоколи, алгоритми забезпечення безпеки. Можливе використання різних механізмів підтримки якості обслуговування при встановленні з'єднання між абонентами різних операторів. З цих причин, підсистема забезпечення якості та підсистема забезпечення безпеки IP-телефонії вимагають більш детального вивчення [1].

1.2 Забезпечення якості в IP-телефонії

1.2.1 Показники якості IP-телефонії

Міжнародний союз електрозв'язку (МСЕ) визначає якість надаваних послуг як "сумарний ефект показників якості послуги, який визначає ступінь задоволеності користувача послуги" [13].

Найбільш популярним з показників якості IP-телефонії є оцінка MOS (Mean Opinion Schore), яка визначається як середнє значення оцінок якості по п'ятибальною шкалою, отриманих великою групою слухачів-експертів.

Якість IP-телефонії такими двома складовими - якістю мови і якістю сигналізації [1]. Якість мови включає в себе:

• діалог - можливість користувача зв'язуватися і розмовляти в реальному часі в повнодуплексному режимі з іншим користувачем;

• розбірливість - чистота і тональність мови;

• луна - чутність власної мови;

• рівень - гучність мови. Якість сигналізації включає:

• затримки при встановленні виклику - швидкість успішного доступу і час встановлення з'єднання;

• завершення виклику - час відбою і швидкість роз'єднання;

• DTMF - визначення і фіксація сигналів многочастотного набору номера.

При використанні захищеної IP-телефонії додатково з'являються показники:

• час виконання з'єднання тобто час встановлення захищеного голосового каналу між кореспондентами, які використовують протоколи розподілу ключів;

• ймовірність успішної атаки порушника на IP- телефонію, що працює в захищеному режимі;

• час і ймовірність успішного завершення протоколів забезпечення безпеки.

IP-телефонія стає масовим явищем в наш час, тому на неї так само можуть поширюватися норми, що пред'являються до традиційної телефонії.

Для контролю показників якості IP-телефонії необхідно враховувати дві сукупності норм: норми, поширюються на пакетні канали зв'язку, а також норми, що поширюються на телефонію.

Для мережі передачі даних виділяють наступні показники:

1. Втрати - відношення коректно прийнятих пакетів до загальної кількості переданих пакетів.

2. Затримки - час, який потрібен для передачі пакета від точки відправлення до точки отримання.

3. Пропускна здатність - доступна для передачі між кореспондентами смуга пропускання.

4. Коливання затримки - різниця між затримками, що виникли при передачі різних пакетів.

Для мережі передачі даних для різних класів трафіку в рекомендації МСЕ-Т Y.1541 вводяться норми на середню затримку [13], варіацію затримки, коефіцієнт втрачених пакетів, коефіцієнт помилок в прийнятому пакеті. Норми представлені в табл. 1.1.

В рекомендації G.114 для телефонної мережі сформовані нормативи на односторонню затримку [14].

Параметр не повинен перевищувати 400 мс при мережевому плануванні. У документі наведено деякі значення затримок, які рекомендується використовувати в розрахунках при використанні різних середовищ передачі і гібридних каналів передачі даних.

Таблиця 1.1 - Норми за рекомендацією МСЕ-Т Y.1541

Характеристики мережі	Класи якості обслуговування (QoS)					
	0	1	2	3	4	5
Затримка доставки пакета IP, IPTD (мс)	100	400	100	400	1000	--
Варіація затримки пакета IP, IPDV (джиттер) (мс)	50	50	--	--	--	--
Коефіцієнт втрати пакетів IP, IPLR	10^{-3}	10^{-3}	10^{-3}	10^{-3}	10^{-3}	--
Коефіцієнт помилок пакетів IP, IPER	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}	--

У законодавстві в галузі зв'язку слід виділити наказ Міністерства інформаційних технологій і зв'язку від 27 вересня 2007 р N113 "Про затвердження Вимог до організаційно-технічного забезпечення стійкого функціонування мережі зв'язку загального користування" [17]. Документ описує кількісні вимоги до показників якості для місцевих, міжнародних і міжміських викликів.

У наказі нормуються і визначаються такі показники:

• частка відбулися викликів;

• час з початку передачі інформації про заняття лінії до отримання відповіді від станції – час відгуку вузла станції;

• час з моменту закінчення набору номера до отримання сигналу про стан обладнання абонента - час встановлення з'єднання;

• час з моменту отримання обладнанням абонента від вузла зв'язку інформації про відповіді користувацького обладнання абонента до моменту встановлення між користувачами з'єднання по голосовому каналу - час на виконання з'єднання;

• час роз'єднання.

Показники мають різне значення в залежності від охоплення мережі зв'язку. У табл. 1.2 наведені значення нормованих параметрів, описаних в нормативному документі. Для досягнення високих показників якості застосовують декомпозицію мережі на кілька конструктивних блоків і використовують додаткові способи і алгоритми в кожному з них. Далі вони розглянуті більш докладно.

1.2.2 Методи забезпечення якості в VoIP

В рекомендації ITU-T Y.1291 виділяється кілька основних конструктивних блоків [15], розподілених за трьома площинах (рис. 1.3).

• Площина управління, що містить механізми управління трактами, через які проходить трафік користувача. До складу цих механізмів входить управління допуском, маршрутизація для QoS і резервування ресурсів.

• Площина даних містить механізми, що працюють безпосередньо з трафіком користувача. До складу цих механізмів входить управління буферами, запобігання перевантаження, маркування пакетів, організація черг і диспетчеризація, класифікація трафіку, правила його обробки та моделювання.

• Площина адміністративного управління, що містить механізми, які стосуються експлуатації, адміністрування і адміністративного управління мережею. До складу цих механізмів входять: угода про рівень обслуговування (SLA), відновлення трафіку, вимір і реєстрація, а також задані правила доставки інформації

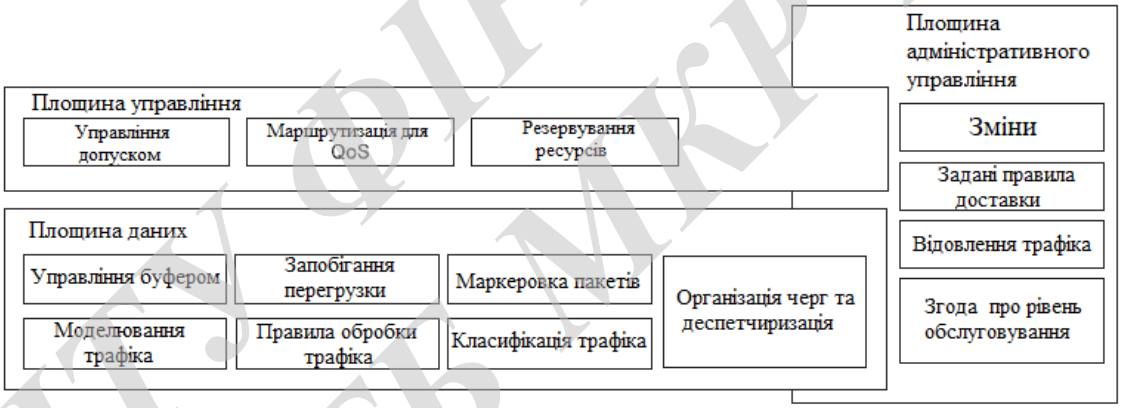


Рисунок 1.3 - Архітектурна модель для підтримки QoS за рекомендацією ITU-T Y.1291

Далі будуть розглянуті протоколи і методи забезпечення якості, що застосовуються в різних площинах архітектурної моделі для підтримки QoS. У площині даних виконуються класифікація і маркування пакетів, застосовуються планування до пакетів, а також використовуються додаткові алгоритми обробки пакетів.

Класифікація може виконуватися в залежності від CoS, MPLS-EXP, номера порту підключення кореспондента до мережевого обладнання або MAC адреси відправника або одержує, Ethertype відправляється пакета та інших ознак. Основним завданням класифікації є поділ пакетів на групи з метою їх подальшої маркування з призначенням параметрів пакету:

• MPLS-EXP - три біта в MPLS для маркування QoS;

• біти CoS 802.1p;

• IP Precedence байт (ToS) або DSCP.

Інструмент планування застосовується для визначення який кадр або пакет буде першим виходити з інтерфейсу мережевого вузла. Завдання вирішується за рахунок застосування алгоритмів управління чергою, а також механізмів запобігання переповнення черги. Виділяють алгоритми управління чергою: SP, WRR, WFQ, CBWFQ, MDRR, LLQ (PQ + CBWFQ), WRED.

Детальний розгляд кожного з алгоритмів виходить за рамки дослідження.

Опис алгоритмів приведено в [49]. найбільш поширеним є застосування пріоритетності голосового трафіку в низькошвидкісних бездротових каналах зв'язку (КС) [50].

Для забезпечення якості VoIP можуть застосовуватися механізми обмеження швидкості - policing або shaping. Policing - обмеження швидкості передачі даних без буфера. Shaping - обмеження швидкості передачі даних з проміжним буфером.

Додатково може застосовуватися управління потоком Ethernet - механізм, що дозволяє попередити відправника про необхідність зупинити передачу даних на зазначеному інтервалі часу з причини, що приймає порт не може виконати обробку.

Для низькошвидкісних каналів додатково можуть бути застосовані механізми:

• Фрагментація і чергування пакетів;

• Механізми компресії (Compressed RTP - cRTP).

Так cRTP дозволяє стискати заголовок голосового пакету IP / UDP / RTP з 40 до 2-5 байт. Однак - даний механізм використовується тільки в межах одного фізичного каналу зв'язку.

До механізмів площині управління архітектурної моделі для підтримки QoS відносяться застосування RSVP (резервування ресурсів) на мережі, а також використання алгоритмів маршрутизації з урахуванням QoS. В якості вхідних даних алгоритми можуть використовувати значення полів в промаркованих пакетах і таблицю маршрутизації, що враховує різні параметри QoS для інтерфейсів обладнання і для різних маршрутів. частина такого функціоналу підтримується, наприклад, протоколом маршрутизації OSPF. Механізми маршрутизації з урахуванням вимог QoS і додаткових можливостей протоколу OSPF описані в RFC 2676 [15].

До площині адміністративного управління відносяться механізми зміни параметрів для VoIP трафіку, які застосовуються на призначених для

користувача терміналах, IP-телефонних станціях, а також на додаткових елементах мережі VoIP, таких, як RTP-проксі-сервери і прикордонні контролери сесій (SBC, Session Border Controller).

1.2.3 Методи оцінки якості VoIP і стан досліджень

У світі ведуться активні дискусії про те, які моделі використовувати для оцінки якості сервісів, а також як оцінити ефективність обробки пакетів в мережі, які методики використовувати для оцінки якості послуг, що надаються.

Ведуться активні розробки в напрямку оцінки QoS і QoE VoIP трафіку. QoS (Quality of Service - Якість Обслуговування) за визначенням ITU - це колективний ефект роботи сервісів, який визначає ступінь задоволення користувача обслуговуванням.

QoE (Quality Of Experience - Якість сприйняття) суб'єктивна міра оцінки роботи системи.

QoE покладається на людське думка і відрізняється від якості обслуговування QoS, яке може бути точно виміряна. Наприклад, реакція людини при прослуховування музики через навушники базується не тільки на частотній характеристиці системи і спікерів, а й на комфорті одиниці, чутливості слуху людини.

Для IP-телефонії MCE стандартизував математичну модель в рекомендації G.107 для оцінки QoE виходячи з параметрів якості терміналу і мережі. Ця модель отримала назву E-model і служить для розрахунку R-фактора [18].

Модель була широко використана для оцінки QoE в мережах IP-телефонії в Японії. Така ж модель була необхідна для сервісів відеотелефонії. В результаті в лабораторії NTT був розроблений набір параметрів для оцінки сприйняття якості відеотелефонії, які згодом використовувалися в новій моделі MCE для відеотелефонії.

Використовуючи Е-модель, а також параметри каналу передачі даних і параметри застосовуваної системи IP-телефонії, можна оцінити MoS (Mean Opinion Score) - суб'єктивний рівень якості, що сприймається користувачем послуги IP-телефонії. В рекомендації [19] наводиться відповідність R-фактора, описуваного і обчислюється з використанням Е-моделі, і параметра MoS (табл. 1.2).

На підставі табл. 1.2 обрана нижня межа MOS 3.6, якій відповідає R = 70.

Необхідно визначити можливі параметри каналу зв'язку - затримку в каналі зв'язку (d) і% втрати пакетів (p.l.) - при яких буде досягатися значення R70.

Таблиця 1.2 - Зв'язок R-фактор та MoS за рекомендаціями G.107

R-фактор	MoS (нижній поріг)	Задоволеність користувачів
90	4,34	Висока задоволеність
80	4,03	Задоволеність
70	3,60	Деякі користувачі не задоволені
60	3,10	Багато користувачів не задоволені
50	2,58	Майже всі користувачі не задоволені

В [20] розглядається вплив параметрів каналу зв’язку на надану якість послуг VoIP для різних кодеків: G.711, G.723 та G.729. Для цього виконується розрахунок MoS з використанням E-моделі для різних затримок каналу зв’язку в інтервалі затримок 0-1200 мс, а також для втрат пакетів 0-12%. На рис. 1.4-1.6 видно, як змінюється R в залежності від p.l. і від d. Додатково на графіках відмічено умови, при яких забезпечується значення R≥70.

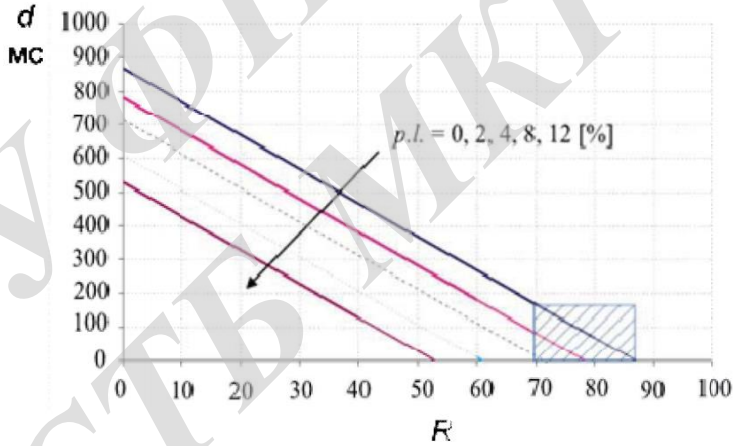


Рисунок 1.4 – Залежність R-фактора від втрати пакетів і затримки в каналі зв’язку для кодека G.723

Із рис. 1.4 - 1.6 видно, що кодек G.711 забезпечує найбільше значення MoS при найгірших умовах в каналі зв’язку: максимальній затримці і втраті пакетів. При p.l.=0 умова R≥70 виконується для d≤300 мс, при p.l.=12, R≥70 виконується для d≤100 мс.

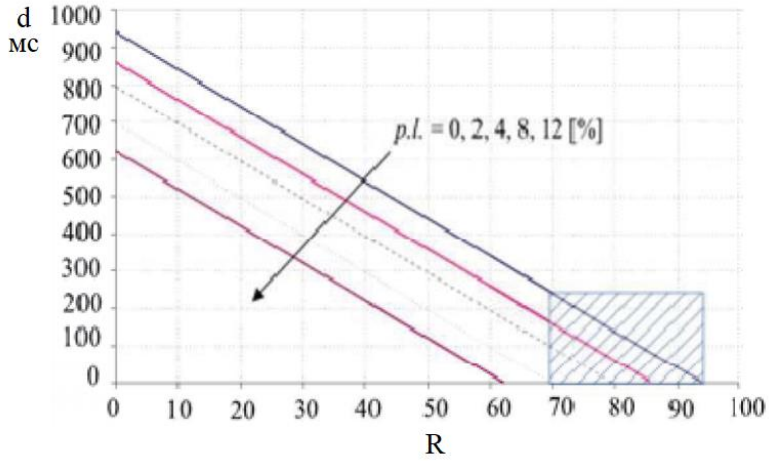


Рисунок 1.5 – Залежність R-фактора від втрати пакетів і затримки в каналі зв’язку для кодека G.729

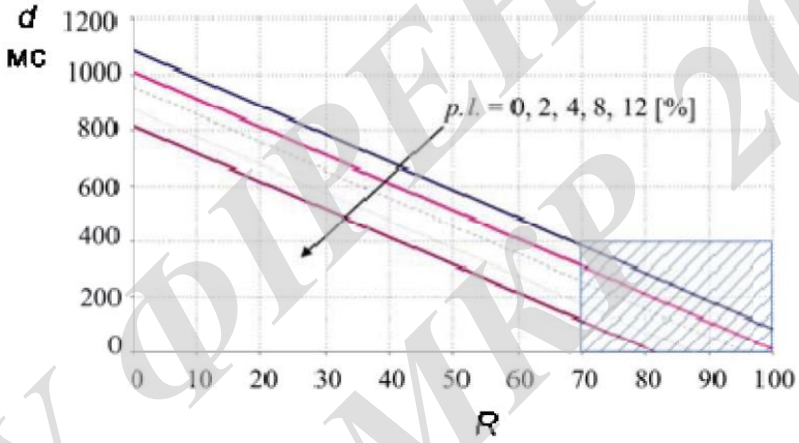


Рисунок 1.6 – Залежність R-фактора від втрати пакетів і затримки в каналі зв’язку для кодека G.711

Подальший аналіз протоколів забезпечення безпеки доцільно проводити для каналу зв’язку з параметрами $d \leq 300$ мс і p.l. = 12 при використанні кодека G.711. В наступних обчисленнях також перевага надається кодеку G.711, як самому стійкому при роботі по каналам зв’язку з помилками.

В якості вхідного параметра при розрахунках замість параметра p.l. зручно використовувати похідний параметр - ймовірність бітової помилки в каналі зв'язку p_0. Для цього необхідно визначити значення p_0, еквівалентну p.l. = 12 для кодека G.711.

$$p.l. = 1 - (1 - p_0)^{ps}, \tag{1.1}$$

де ps - розмір пакета, біт.

Для кодека G.711 допускаються розміри корисного навантаження 80, 160, 240 байт. При цьому розмір пакета з урахуванням заголовків становитиме відповідно 138, 218, 296 байт. p_0 визначається за формулою:

$$p_0 = 1 - 10^{\frac{\lg(1-p.l.)}{ps}}. \quad (1.2)$$

Розраховані значення наведені в табл. 1.3. З таблиці видно, що максимальне значення ймовірності бітової помилки ppl = 12% відповідає $p_0 = 1{,}16 \cdot 10^{-4}$. Відповідно, розрахунки необхідно виконувати для значень $p_0 \leq 1{,}16 \cdot 10^{-4}$.

Таблиця 1.3 - Залежність p_0 від p.l. для кодека G.711

Імовірність втрати пакету, p.l.	Розмір пакета, ps, біт	Імовірність бітової помилки, p_0
0,12	138	$1{,}16 \cdot 10^{-4}$
0,12	218	$7{,}33 \cdot 10^{-5}$
0,12	298	$5{,}36 \cdot 10^{-5}$

В області дослідження методів забезпечення якості при передачі медіа трафіку в Росії ведуться різні дослідження. Над проблемами якості обслуговування і аналізом трафіку в VoIP мережах також працювали док. Сухов А. М. [16], к.т.н. Аль-Шрайдех Халед Садек, маг. Федосєєва О. С. [18], маг. Карімжанова А.С [55], Малаховський А.А., Личагіна Н.І., Гузар А.С. [19] та інші. Так згадуваним вище Суховим А.М була розроблена аналітична модель трафіку на ділянці високошвидкісної мережі (рис. 1.7), згідно з якою для порівняння якості з'єднань в глобальній мережі досить використовувати єдиний параметр: середню швидкість потоку. Імовірнісні характеристики протоколу SIP досліджувалися в роботі Нсангу М. М. [24].

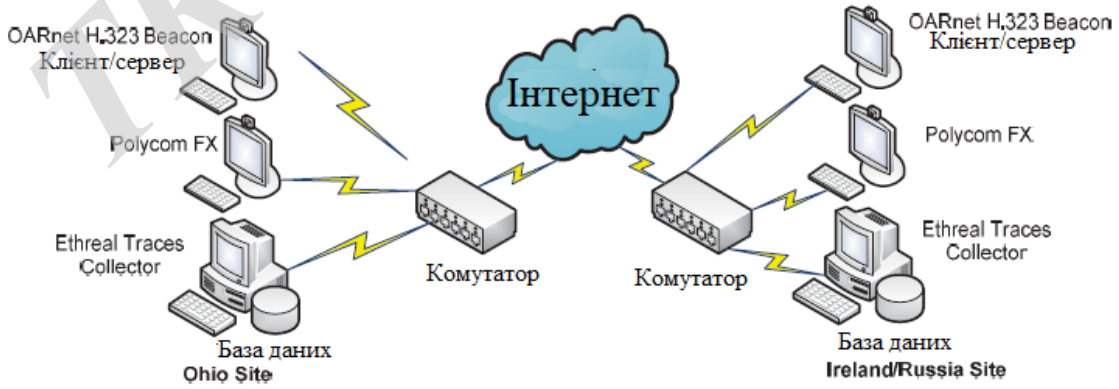


Рисунок 1.7 - Схема експерименту в глобальній мережі док. Сухова А. М.

Тема забезпечення QoS широко обговорюється за кордоном в університетах Центральної Флориди (Erol Gelenbe, Chair Professor, Ricardo Lent, doctor та ін) [19], Карленгтонском університеті Канади (Lijing Ding, Ayman Radwan, Mohamed Samy El-Hennawey [20], Rafik A. Goubran, Ph.D., P.Eng) і ін.

Питання забезпечення QoS розглядається такими організаціями як MCE, IETF, IEEE, ETSI, 3GPP. Були прийняті ряд стандартів для якості QoS IP-телефонії і моделей щодо забезпечення якості IP-телефонії, але до теперішнього часу не існує єдиного стандарту. Однак, питання впливу протоколів забезпечення безпеки на якість вивчені вкрай слабо і вимагають опрацювання та оцінки.

1.3 Забезпечення інформаційної безпеки IP- телефонії

В силу загальнодоступності використовуваних каналів передачі голосової інформації в IP мережах особливої актуальності набуває забезпечення конфіденційності VoIP-сервісів.

Для вирішення цього завдання можуть бути використані різні підходи:

- забезпечення прямого захищеного каналу між кореспондентами (Наприклад, VPN-тунель);
- застосування спеціальних протоколів забезпечення безпеки для IP-сервісів.

Перший спосіб набув широкого поширення при побудові віртуальних корпоративних мереж, але для його реалізації кореспонденти повинні підтримувати VPN-протокол. Однак, багато VoIP-пристрої не підтримують VPN (табл. 1.4).

Тому, для забезпечення безпеки досить часто застосовуються спеціальні протоколи забезпечення безпеки IP-телефонії.

Таблиця 1.4 - Продукти захищеної IP-телефонії

Виробник	Продукт	Реалізація	Протокол захисту			Підтримка VPN
			Встановлення з’єднаня	Медіа-трафіка	Розділення ключів	
LinkSys	SPA8000	апаратна	SIPS / TLS	SRTP	Немає даних	Ні

LinkSys	Cisco SPA112	апаратна	SIPS / TLS	SRTP	Немає даних	Ні
Dlink	DVG-5008S	апаратна	немає даних	немає даних	немає даних	PPTP
AddPack	AP200	апаратна	SIPS / TLS	SRTP	немає даних	немає даних
Grandstream	GXW400x	апаратна	SIPS / TLS	SRTP	SDES	Ні
UM-Labs	RC-2100	апаратна	SIPS / TLS	SRTP	ZRTP, SDES	немає даних
CounterPath	Eye-beam	програмна	SIP / TLS	SRTP	TLS	ні
3XC	3CX softphone	програмна	SIP / TLS	SRTP	даних немає	ні
Asterisk	IP PBX	програмна	SIP / TLS	SRTP	ZRTP	Ні
FreeSwitch	IP PBX	програмна	SIP / TLS	SRTP	SDES	Ні
Phoner	Phoner softphone	програмна	SIP / TLS	SRTP	ZRTP	Ні

1.3.1 Протоколи забезпечення безпеки IP-телефонії

До спеціальних протоколів забезпечення безпеки IP-телефонії відносяться протоколи Secured SIP, SRTP, MIKEY, SDES, ZRTP, DTLS, S-MIME. Ці протоколи можна розділити на 3 категорії [8]:

• Протоколи захисту сигналізації (Secured SIP);

• Протокол захисту медіаінформації (SRTP);

• Протоколи генерації і розподілу ключів для протоколів захисту медіаінформації (MIKEY, SDES, ZRTP, DTLS).

Необхідно розглянути докладніше ці категорії.

Протоколи захисту сигналізації призначені для забезпечення безпеки інформації про телефонні номери що викликає і викликаний абонента, підтримуваних кодеках. Для вирішення цього завдання використовується Secured SIP (SSIP, SIP / TLS) [22]. Цей протокол працює за аналогією з протоколом HTTPS, організовуючи між кореспондентом і сервером SSL тунель з використанням сертифікатів і відкритого ключа. Всі SIP-повідомлення (Сигналізація) передаються з цього тунелю. Недоліком протоколу є необхідність застосування інфраструктури відкритих ключів, що використовується для організації TLS.

Для забезпечення конфіденційності при передачі мови широко використовується захищений протокол реального часу - Secure Real-time

Transport Protocol (SRTP), який реалізує функції криптографічного захисту - шифрування і аутентифікації мовних повідомлень на основі алгоритму шифрування AES.

Криптографічний захист пакетів голосової інформації виконується протоколом SRTP в режимі реального часу і не вносить змін в ймовірносно-часові характеристики протоколу RTP. Але для його роботи необхідно попереднє формування криптографічних ключів. Цю завдання вирішує протокол розподілу ключів (ПРК).

Рекомендація RFC 3711 описує дві складових - власне протокол SRTP для перенесення і криптозахисту медіа даних, а також протокол SRTCP (Secure Real-time Transport Control Protocol) для управління медіа сесією.

Основними завданнями протоколу SRTP є виконання наступних функцій:

• шифрування переданих голосових даних;

• аутентифікація переданих повідомлень;

• захист від передачі повторних пакетів;

• збереження смуги пропускання, стиснення RTP заголовків.

Основними завданнями протоколу SRTCP є виконання наступних функцій:

• шифрування переданих даних;

• аутентифікація переданих повідомлень.

Аутентифікація і шифрування можуть працювати незалежно один від одного. Таким чином, можливий варіант, коли шифрування вимкнено і SRTP застосовується тільки для цілей аутентифікації. Обмеженням протоколу є те, що аутентифікація повідомлення обов'язкова в SRTP і не може бути відключена.

1.3.2 Протоколи генерації і розподілу ключів для захисту медіаінформації

Протоколи третьої групи, за аналогією з родинними протоколами розподілу ключів в бездротових мережах, призначені для генерації і розподілу між кореспондентами ключів шифрування медіаінформації. Для вирішення цього завдання можуть використовуватися протоколи MIKEY, SDES, ZRTP, DTLS.

MIKEY має кілька режимів роботи, що визначають спосіб формування секретного ключа сесії SRTP: режим встановленого ключа, режим відкритого ключа та режим Діффі-Хелмана. Причому другий і третій режими не захищають від атаки вторгнення в середину (MiTM, Man In the Middle) і

вимагають реалізації механізму аутентифікації повідомлень. Транспортом для переносу повідомлень протоколу може виступати як SIP / SDP, так і протокол RTSP (Real Time Streaming Protocol). SDES (Session Description Protocol Security) описується в RFC4568. суть протоколу полягає в тому, що один з кореспондентів передає ключ в SIP повідомленні по сигнальному каналу [23].

Кореспондент отримує його і використовує для шифрування. Однак при цьому обмін сигнальними повідомленнями повинен бути захищений від зловмисника. З цієї причини - SDES може використовуватися тільки при наявності SIP / TLS захищеного з'єднання з цифровим сертифікатом сервера.

Також даний спосіб не забезпечує безпеки з кінця в кінець. Це означає, що якщо з'єднання буде виконуватися через IP АТС, SDES буде виконувати розподіл ключів між кореспондентом А і IP PBX, між кореспондентом Б і IP-телефонною станцією, але не між кореспондентами А і Б безпосередньо.

Протокол DTLS для SRTP описується в RFC 5764. Протокол описує формування медіа-сесій точка-точка з двома учасниками з жорстким фіксуванням портів UDP кореспондента і респондента [23]. Повідомлення протоколу передаються спільно з RTP пакетами.

Кожна сесія містить одну DTLS асоціацію і два SRTP контексту (для SRTP і SRTCP). Для організації сесії (DTLS-асоціації) кореспонденти виконують обмін повідомленнями, званий DTLS handshake (рис. 1.8) Так як в основі протоколу лежить TLS, використовує інфраструктуру відкритих ключів (Public Key Infrastructure, PKI), то застосування TLS можливо теж тільки при наявності PKI.

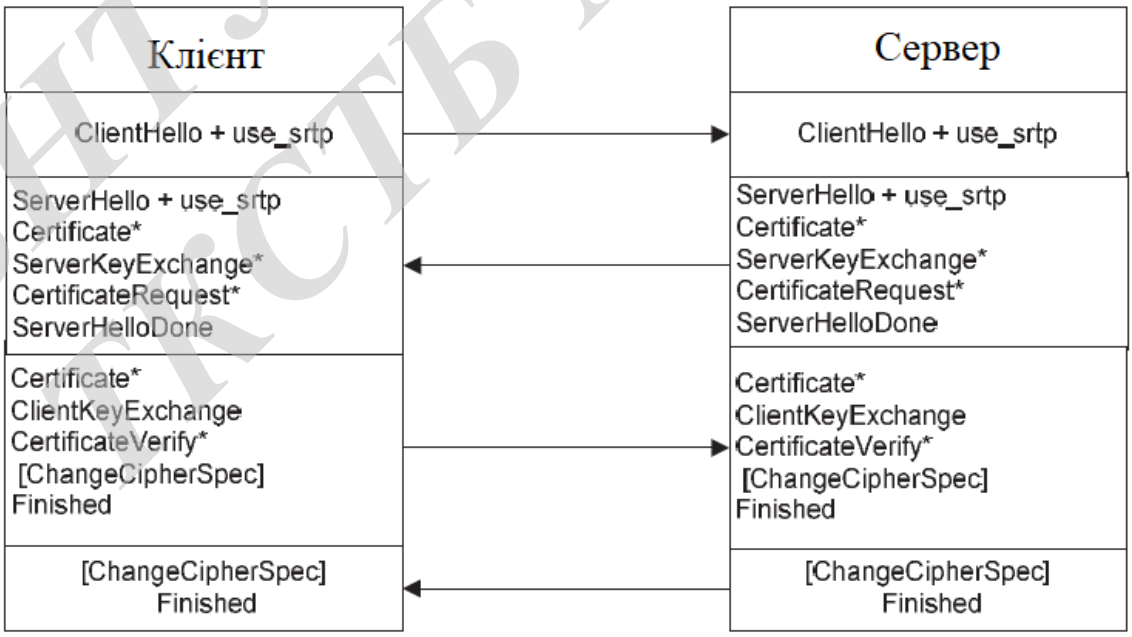


Рисунок 1.8 - Обмін повідомленнями DTLS

Одним з найбільш перспективних протоколів генерації ключів є ZRTP. Протокол застосовується в додатку для Android CsipSimple, програмних телефонах Jitsi, Phoner, програмних АТС FreeSwitch і Asterisk, апаратних VoIP шлюзах компанії UM-Labs.

Відмінною особливістю ZRTP протоколу є можливість забезпечення безпеки з кінця в кінець, від одного кореспондента до іншого. Завданнями протоколу ZRTP є:

• генерація ключових параметрів SRTP сесії;

• забезпечення конфіденційності повідомлень протоколу;

• забезпечення аутентифікації кореспондентів;

• захист від атаки вторгнення посередині, як з використанням, так і без використання інфраструктури відкритих ключів.

Протокол передбачає роботу кореспондентів по топології точка-точка, при цьому окремо виділяється можливість застосування протоколу при багатопотоковому режимі, коли необхідно організувати кілька захищених медіа потоків. Крім того, передбачений режим роботи з легітимним посередником, яким може бути, наприклад, корпоративна телефонна станція. Кожен з кореспондентів-учасників протоколу повинен мати встановлений ідентифікатор (ZID), який повинен бути унікальний.

В основі протоколу - обмін ключами по алгоритму Діффі-Хелмана. Особливістю протоколу є передача параметрів всередині RTP пакетів, залишаючи пакети сумісними з RTP / AVP профілем. В цьому випадку, ZRTP-несумісним пристроєм ZRTP-пакети просто відхиляються і не впливають на встановлене з'єднання.

Для аутентифікації кореспондентів, а також виключення атаки вторгнення в середину (MiTM, Man in The Middle), протокол ZRTP передбачає використання короткої аутентификационной рядки (SAS, Short Authentication String), а також частини ключового матеріалу від попередніх сесій між кореспондентами. Для контролю цілісності переданих повідомлень кожне повідомлення ZRTP включає в себе код CRC, а також код аутентифікації повідомлення MAC (Message Authentication Code). MAC обчислюється, як ключова хеш-функція, яка узгоджується на першій фазі протоколу. Виявлення помилки тільки в хеш-повідомленні, як правило, означає виявлення атаки MiTM, оскільки спотворення за рахунок канальних помилок виявляються і при перевірці CRC ZRTP пакету.

Протокол виконується послідовно в чотири фази:

1. Виявлення;

2. Підтвердження;

3. Обчислення ключів;

4. Завершення.

У загальному випадку, ZRTP працює на самому початку розмови кореспондентів, відразу після завершення роботи протоколу SIP, як починає працювати в сторони протокол RTP (рис. 1.9).

Більш докладно протокол ZRTP описаний в додатку Г.

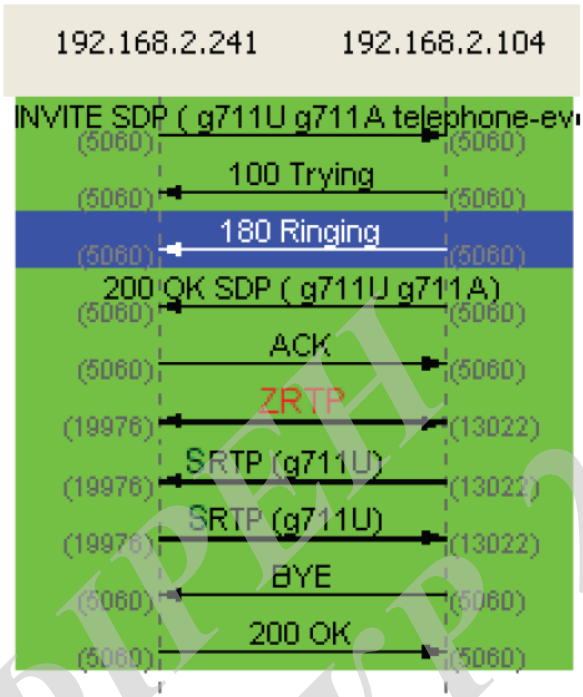


Рисунок 1.9 - Схема обміну повідомленнями між кореспондентами з використанням SIP / SRTP / ZRTP

1.3.3 Вимоги до протоколів розподілу ключів

Для подальшого дослідження також необхідно сформулювати вимоги, яким повинні відповідати ПРК:

1. Протокол повинен підтримувати роботу як в топології клієнт-сервер, так і в топології клієнт-клієнт.

2. Протокол повинен бути самодостатнім і виконувати функцію розподілу ключового матеріалу без застосування додаткових протоколів між кореспондентами.

3. Протокол повинен підтримувати механізм розподілу ключів в топології клієнт-клієнт без передачі ключа в явному вигляді по каналу зв'язку.

4. Протокол повинен мати механізм виявлення MITM без заздалегідь розподіленого ключового матеріалу між кореспондентами.

5. Протокол повинен використовувати TCP / UDP порти, що застосовуються для IP- телефонії, або TCP / UDP порти, використання яких узгоджено в результаті встановлення з'єднання.

Перша вимога обгрунтовано необхідністю забезпечення безпеки в топології клієнт-клієнт, так як в топології клієнт-сервер кореспонденти вже мають перед розподілений загальний секрет, який використовується для захисту повідомлень протоколу розподілу ключів для SRTP

Друга вимога обґрунтовано вимогами по простоті інтеграції в існуючі системи зв'язку, програмні термінали. У разі одночасної роботи кількох протоколів, кожен з яких передає свої повідомлення по каналу зв'язку, це ускладнить інтеграцію протоколу в програмний VoIP термінал користувача.

Третя вимога обгрунтовано принципом забезпечення безпеки, обмовляється, що ключ шифрування ніколи не повинен передаватися по каналу зв'язку в явному вигляді.

Четверта вимога викликано можливістю використання протоколу розподілу ключів між рівноправними кореспондентами, які не мають попередньо розподіленого ключового матеріалу і загальних сертифікатів, а також загального довіреної центру сертифікації.

П'ята вимога викликана спрощенням інтеграції протоколу безпеки в існуючі мережі з метою перешкоди блокування повідомлень протоколу розподілу міжмережевими екранами при використанні TCP або UDP портів, не передбачених протоколами SIP / RTP.

1.3.4 Стан досліджень щодо захисту голосових зв'язків при використанні IP-телефонії

Існуючі дослідження в області робіт із захисту голосових зв'язків можна розділити на кілька

категорій, а саме:

• розробка безпечних систем IP-телефонії;

• аналіз безпеки, що забезпечується системами IP-телефонії;

• аналіз безпеки, що забезпечується окремими протоколами VoIP, а також аналіз самих протоколів.

До робіт першої категорії відносяться роботи Нопіна С.В. і Шахова В.Г. [21]. вони займалися розробкою програм захищеної IP-телефонії, а також вивченням особливостей захисту голосової інформації. У роботі [23] основним напрямком дослідження було застосування засобів ОС Windows для організації безпечної IP-телефонії, при цьому для розподілу ключів пропонувалося використовувати центри розподілу ключів.

Друга категорія присвячена роботам з аналізу рівня безпеки, який забезпечують сучасні системи безпеки IP-телефонії. До цієї категорії

відносяться роботи, в яких розглядаються загальні питання щодо забезпечення безпеки в системах IP-телефонії: "Забезпечення безпеки сучасних VoIP мереж" [5], "Захист інформації на корпоративних мережах VoIP" [6]. Деякі роботи спрямовані на формування вимог щодо забезпечення безпеки в мережах IP-телефонії. До цих робіт ставитися, наприклад, робота "Методика формування вимог щодо забезпечення інформаційної безпеки мережі IP-телефонії від загроз середньостатистичного «хакера»" [7] Макарової О. С., де запропоновано підхід щодо формування вимог, яким повинна відповідати безпечна VoIP мережу.

До робіт третьої категорії відносяться дослідження, спрямовані на аналіз протоколів забезпечення безпеки VoIP. До цих робіт відносяться дослідження Еммануеля Оніка з університету Олександру Іоана Куза (Румунія). У роботі "Securing the Media Stream Inside VoIP SIP Based Sessions" [9] проводитися дослідження SRTP протоколу та протоколів обміну ключами, наводяться можливі атаки на протоколи, а також описується реалізація інтеграції протоколу ZRTP в програму "SIP Communicator". Відомо кілька робіт , [10] з аналізу протоколів на наявність вразливостей, наприклад в «ProVerif Analysis of the ZRTP Protocol» проводитися аналіз протоколу ZRTP на наявність вразливостей за допомогою моделювання в програмі ProVerif. У дослідженні наводиться опис декількох атак на VoIP протоколи, в тому числі атак на MIKEY і SDES протоколи.

У роботі "Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations" досліджується застосування протоколу SRTP при роботі з кодеками зі змінною швидкістю кодування. Показано, що інформація про довжину зашифрованих VoIP пакетів може бути використана для ідентифікації фраз, вимовлених в розмові. Дослідження показало, що пасивний супротивник може ідентифікувати фрази з стандартного діалогу, в зашифрованому телефонної розмови, зі середньої точність 50%, і з точністю понад 90% для деяких окремих фраз.

Дослідження в області атак MITM і методів захисту від них наводяться в роботах Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Багдасарян Р.Х. [11], Canteaut A. [12], Sun H., Song J., Chen Z. [13], Радивилова Т.А., Бушманова В.С. [14], Карпухіна Е.О., Михайлова В.Ю. [15].

При цьому небезпека і поширеність даної атаки найбільш активно відзначається в різних джерелах масової інформації. Однак жодна з робіт не досліджує ймовірносно-часових характеристики протоколів забезпечення безпеки VoIP.

1.4 Постановка наукових завдань дослідження МКР

При оцінці впливу протоколів забезпечення безпеки на якість потрібно враховувати особливості IP-телефонії в порівнянні з традиційною телефонією. Так, у традиційній телефонії час відгуку вузла зв'язку, тобто час з початку передачі інформації про заняття абонентської лінії до моменту отримання кінцевим обладнанням сигналу готовності до прийому номера, визначається готовністю станції обслужити виклик. В IP-телефонії це час визначається кінцевим обладнанням і не залежить від поточного стану телефонної станції. Однак, параметр "час встановлення з'єднання" для IP- телефонії включає в себе час відгуку вузла IP-телефонної станції, а також час, необхідний для взаємодії між кореспондентами, або кореспондентом і телефонною станцією.

Відлік цього часу починається після закінчення набору номера користувачем і закінчується отриманням сигналу очікування відповіді або зайнятості від респондента.

Необхідно оцінити, як протоколи безпеки IP-телефонії можуть впливати на нормовані показники функціонування мереж телефонної мережі зв'язку. Застосування SIP-S може впливати на норму "втрати викликів" в разі, якщо при сценарії абонент-абонент один з кореспондентів використовує політику безумовного використання SIP-S, а другий не підтримує SIP-S протокол. Деяка затримка додатково може виникати за рахунок часу, необхідного на організацію TLS каналу між кореспондентами, необхідного для роботи SIP-S протоколу.

Протоколи розподілу ключів впливають на час встановлення з'єднання або на час організації захищеного мовного каналу, в залежності від місця спрацьовування протоколу в сценарії з'єднання. Так протокол ZRTP може працювати після встановлення з'єднання, починаючи з етапу, коли один з кореспондентів зняв трубку. В цьому випадку, протокол впливає на норму "Час встановлення з'єднання". Інші протоколи також вимагають передачу додаткових повідомлень, що може збільшувати значення нормованих параметрів.

Відповідно до вищевикладеного, метою магістерської кваліфікаційної робота роботи є оцінка ймовірносно тимчасових характеристик протоколів безпеки IP-телефонії, як впливають на параметри якості IP-телефонії, а також підвищення безпеки IP-телефонії при роботі кореспондентів в топології клієнт-клієнт без сервера.

Для досягнення мети необхідно вирішити такі наукові завдання:

1. Дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості;

2. Розробка моделі порушника для оцінки захищеності системи IP-телефонії. Розробляється модель дозволить врахувати атаки, які може виконати порушник при використанні декомпозиції безпеки IP-телефонії на складові протоколи.

3. Розробка методики оцінки ймовірнісно-часових характеристик протоколів забезпечення безпеки IP-телефонії, що дозволяє оцінити такі характеристики протоколу, як час успішного завершення і ймовірність успішного завершення при роботі по каналах зв'язку з помилками і затримками з урахуванням особливостей протоколів

4. Розробка пропозицій щодо модифікації протоколу розподілу ключів для поліпшення ймовірносно-часових характеристик протоколу. Модифікація дозволить ПРК працювати по каналах з великими затримками, ніж оригінальні ПРК, при цьому виконуючи встановлені норми.

5. Розробка методу виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана, який дозволить знизити ймовірність успішної атаки НСД;

6. Розробка пропозицій щодо модифікації протоколу Zimmermann Real-time Transport Protocol (ZRTP) для забезпечення безпеки кореспондентів при взаємодії без сервера в топології клієнт-клієнт. Модифікований ПРК дозволить зменшити ймовірність успішної атаки порушника, який контролює канал зв'язку, і може використовуватися для підвищення безпеки у випадках, коли кореспонденти не мають захищеного каналу зв'язку, або термін дії існуючого ключового матеріалу закінчився, або загальний секрет компрометувати порушником.

Відповідно до вищевикладеними цілями і завданнями дослідження магістерська кваліфікаційна робота має назву "Методи підвищення інформаційної безпеки IP-телефонії з урахуванням ймовірносно-часових характеристик протоколів розподілу ключів ".

1.5 Висновки до розділу 1

У першому розділі розглянуті актуальні проблеми та існуючі підходи їх вирішення в області захищеної IP-телефонії. Зокрема, розглянуті основні компоненти і протоколи IP-телефонії, а також можливі сценарії встановлення з'єднань. Описано механізми і алгоритми, що застосовуються для забезпечення нормованого показника MOS, а також значень інших нормованих показників. Показано значення параметрів каналу зв'язку, при яких має сенс виконувати аналіз роботи протоколів IP-телефонії.

Наведено набір протоколів забезпечення безпеки IP-телефонії, а також класифікація протоколів і їх скорочений опис. Виконано огляд досліджень в області забезпечення безпеки IP-телефонії, і виявлено відсутність досліджень щодо впливу протоколів безпеки на нормовані параметри функціонування мережі телефонії. Показано вплив протоколів безпеки на параметри функціонування мережі телефонії, виражене в виникненні затримки при встановленні захищеного з'єднання між кореспондентами.

2 МАТЕМАТИЧНА МОДЕЛЬ АКТИВНОГО ПОРУШНИКА ДЛЯ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ

Порушник може вибрати різні способи атаки на систему IP- телефонії, що працює в захищеному режимі, виходячи з особливостей протоколів забезпечення безпеки IP-телефонії, описаних в розділі 1.3. Існують кілька моделей порушника в IP-телефонії. Імовірнісна модель порушника описана в [3] і описує дії порушника, а також основні атаки при реалізації безпечної IP-телефонії на ОС Windows. Модель враховує різні типи атак, в тому числі, характерні саме для Windows при використанні криптографічних засобів операційної системи. Однак, дана модель не враховує, що ключі поширюються за допомогою протоколів розподілу ключів IP-телефонії, і передбачає тільки попередню установку секрету у обох кореспондентів. При атаці, спрямованої на несанкціонований доступ до інформації (НСД), розглядається тільки ймовірність дешифрування переданого контенту методом перебору, а атака модифікація пакетів розглядається тільки в разі успішної атаки отримання пароля при дешифрування перехоплених пакетів.

У стандарті Російської Федерації, підготовленому Федеральною службою з технічного та експортного контролю, описується загальна модель порушника. Модель також не враховує особливостей роботи безпечної IP-телефонії, що складаються в застосуванні декількох протоколів для забезпечення безпеки: захист сигналізації, захист медіа трафіку, розподіл ключового матеріалу, - а також не описує атаки безпосередньо на ці протоколи. В роботі [7] запропонована сукупність вимог, що пред'являються до мережі IP-телефонії, а також описуються основні загальні типи атак на систему IP-телефонії від середньостатистичного хакера. Однак, в роботі відсутній декомпозиція протоколів безпеки IP - телефонії на складові і відсутній опис атак конкретно на ці протоколи. В роботі [6] описуються загальні принципи забезпечення безпеки, а також можливі дії порушників при атаках на систему IP-телефонії. При цьому не розглядаються атаки на протоколи розподілу ключового матеріалу, використовувані в IP- телефонії. Так як в існуючих моделях порушника [29 - 36], не описується декомпозиція протоколів безпеки IP-телефонії, доцільно розробити нову модель порушника, що враховує описані вище особливості.

Існуючі моделі [1,3,7,6] не дозволяють визначити ймовірність успішної атаки НСД на систему захищеної IP- телефонії, що працює за схемою кореспондент-кореспондент, не враховують атаку людина посередині (MITM) на ПРК. Внаслідок цього доцільно розробити таку модель порушника, яка дозволила б вирішити це завдання.

2.1 Загрози інформаційної безпеки в IP-телефонії

Загроза безпеки інформації в IP-телефонії виникає в результаті утворення каналу між джерелом загрози і носієм (джерелом) інформації, що створює умови для порушення безпеки інформації.

Актуальність загрози безпеки інформації буде визначатися, в тому числі, видом джерела загрози безпеки інформації, наявністю вразливості джерела інформації і середовищем поширення інформаційного сигналу.

По виду джерела загрози впливів на інформацію можна виділити:

• загрози, пов'язані з діяльністю організацій, що володіють високим потенціалом, оснащеністю і мотивацією, зумовленої політичними, економічними, військовими та іншими цілями іноземних держав;

• загрози, пов'язані з діяльністю організацій, що володіють мотивацією, обумовленої їх економічними, інформаційними та іншими цілями;

• загрози, пов'язані з діяльністю окремих фізичних осіб (злочинних елементів).

Способи впливу на інформацію визначаються можливостями джерела загроз. Джерело загроз, приймає дії або здійснює підготовку до дій щодо несанкціонованого впливу на інформацію є порушником інформаційної безпеки.

Далі в якості порушника розглядається фізична особа, випадково або навмисно скоює дії в своїх інтересах або в інтересах організацій, наслідком яких є порушення безпеки інформації при її обробці технічними засобами в інформаційних системах.

Доцільно розглядати порушників з точки зору наявності права постійного або разового доступу в контрольовану зону (КЗ). Виділяється два типи порушників:

• порушники, які не мають права доступу в КЗ - зовнішні порушники;

• порушники, які мають право доступу в КЗ - внутрішні порушники.

Зовнішніми порушниками можуть бути:

• представники розвідувальних служб іноземних держав;

• представники терористичних і кримінальних структур;

• сторонні особи.

Внутрішніми порушниками можуть бути:

• працівники оператора;

• працівники сторонніх організацій - розробників або постачальників програмного забезпечення і технічних засобів, що забезпечують супровід цих коштів на об'єкті, що підлягає.

Забезпечення безпеки передачі мови в IP-телефонії здійснюється із застосуванням криптографічних протоколів: захищеного протоколу реального часу - SRTP, що реалізує функції криптографічного інкапсуляції даних, а також протоколів, що виконують функцію автоматичного розподілу ключів для сесій SRTP, і протоколів захисту сигналізації.

З огляду на, що передача даних IP-телефонії здійснюється по мережах загального доступу, а VoIP термінали доступні будь-якій фізичній особі, як і легальний доступ до мереж - можна зробити висновок про актуальність загроз віддаленого доступу і можливості їх реалізації як зовнішніми порушниками, так і окремими категоріями внутрішніх порушників.

2.2 Узагальнена модель порушника

Під моделлю порушника розуміється опис сукупності практичних і теоретичних можливостей, знань, часу, місця дії, а також інших характеристик, властивих порушнику.

Під ймовірнісної моделлю [stochastic, probabilistic model] - розуміють модель, яка на відміну від детермінованої моделі містить випадкові елементи. При завданні на вході моделі деякої сукупності значень, на її виході можуть виходити розрізняються між собою результати в залежності від дії випадкового фактора.

Під математичною моделлю порушника розуміється модель, яка містить випадкові елементи у вигляді ймовірностей успішного виконання окремих атак, які формують одну загальну атаку, і визначає ймовірність досягнення кінцевої мети цієї атаки порушником.

Щоб модель порушника була максимально корисною - вона повинна орієнтуватися на конкретний об'єкт захисту. Тому модель не може бути універсальною і синтезується виходячи з аналізу структури системи, ресурсів і способів їх використання.

Існуючі моделі порушника не враховує особливостей роботи безпечної IP-телефонії, що складаються в застосуванні декількох протоколів для забезпечення безпеки, а також не описують атаки безпосередньо на ці протоколи.

Отже, доцільно розробити модель порушника, що враховує ці особливості. Для цього необхідно розглянути схему взаємодії кореспондентів захищеної IP-телефонії для прямого з'єднання клієнт - клієнт, при відсутності попередньо розподіленого ключового матеріалу, і можливі варіанти дії порушника в схемі (рис. 2.1).

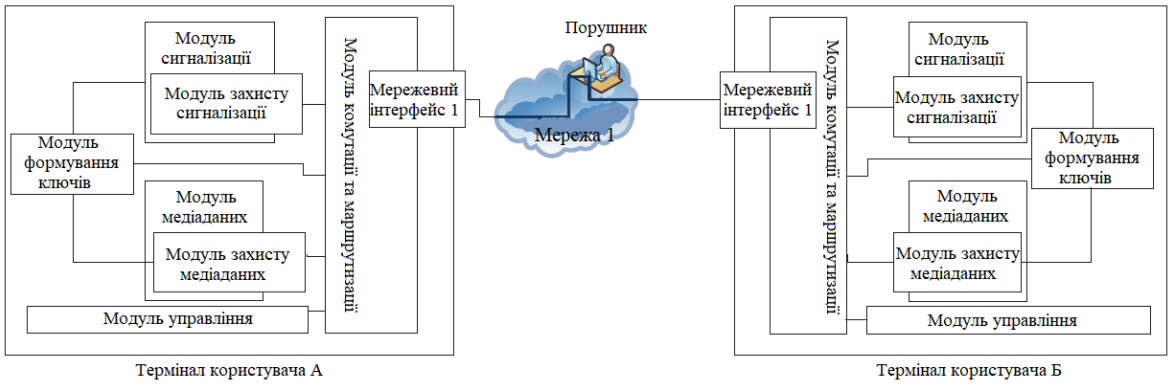


Рисунок 2.1 - Структурна схема з'єднання в сценарії клієнт-клієнт

Порушник може використовувати такі стратегії:

• Пасивну, використовуючи тільки перехоплення переданих даних.

• Активну, використовуючи штатні засоби системи захисту і її недоліки для проведення атаки або додаткові кошти для впливу на систему с метою виконання атаки.

Надалі розглядається порушник, який використовує активну стратегію атаки, яка експлуатує уразливість протоколу Діффі-Хелмана, що лежить в основі більшості протоколів розподілу ключів (ПРК) IP- телефонії. Цей протокол захищає від атаки пасивного порушника. Однак, він нестійкий до атаки Man In The Middle (MITM) активного порушника [24].

При здійсненні протиправних дій порушник може:

• перебувати в одній підмережі з об'єктом атаки, в тому числі мати права доступу будь-якого рівня в мережу або до обладнання, на яке виконується атака;

• не перебувати в одній підмережі з об'єктом атаки або не мати прав доступу будь-якого рівня в мережу або до обладнання, на яке виконується атака.

VoIP терміналом користувача, як правило, є IP-телефон, шлюз IP-телефонії, або інше обчислювальний пристрій (стаціонарний комп'ютер або мобільний термінал: ноутбук, планшетний комп'ютер, смартфон і т.д.) з встановленим спеціалізованим програмним забезпеченням IP-телефонії. Цей пристрій дозволяє користувачеві отримувати послуги IP-телефонії і виконувати аудіо або відео виклики інших користувачів.

При розгляді атак на термінал користувача введено допущення, що в одній підмережі з жертвою може перебувати тільки внутрішній порушник. Відповідно, деякі типи атак будуть доступні тільки для цієї категорії порушників.

Для досягнення цілей НСД порушник при проведенні атаки може використовувати такі існуючі загрози безпеці:

1. Навмисний несанкціонований доступ на обладнання оператора або користувача, отриманий за рахунок атаки перебору пароля або іншої атаки на механізми забезпечення безпеки інформаційної системи (ІС), з боку внутрішніх або зовнішніх порушників, що володіють правами і повноваженнями на доступ до обладнання нижчого рівня, або які не мають доступу до нього.

2. Умисне вплив на таблицю маршрутизації з боку зовнішніх або внутрішніх порушників, а також використання штатних засобів обладнання для часткового перенаправлення трафіку користувачами, що володіють правами і повноваженнями на доступ до інформації в інформаційній системі.

3. Умисне спеціалізоване вплив на обмін повідомленнями ПРК, а також на інші дані, що передаються кореспондентів, спрямоване на порушення конфіденційності і цілісності переданих даних, з боку внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями на доступ до інформації в ІС.

4. Спеціальний вплив у вигляді атаки на шифр на перехоплену інформацію, передану між кореспондентами, з боку внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями на доступ або перехоплення зашифрованої інформації в інформаційній системі, з метою порушення конфіденційності і дешифрування даних.

5. Умисне несанкціоноване спеціальна дія на програмне забезпечення одного або декількох кореспондентів з боку внутрішніх або зовнішніх порушників, що володіють правами і повноваженнями на доступ до обладнання та використовуваному програмному забезпеченню користувача.

6. Навмисна несанкціонована установка додаткового обладнання на вузлі оператора для цілей спеціального впливу на передану від користувачів інформацію з боку внутрішніх порушників, що володіють правами і повноваженнями доступу на вузол оператора.

7. Умисне несанкціоноване вплив на конфігураційні файли терміналу з боку внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями доступу до терміналу користувача, з метою зміни налаштувань безпеки.

8. Навмисний несанкціонований перехоплення авторизаційних даних для управління обладнанням користувача з боку внутрішніх порушників, що володіють правами і повноваженнями на доступ до даних, що передаються між комп'ютером користувача і терміналом користувача.

Для побудови математичної моделі порушника виконаний аналіз загроз і їх джерел. Використовуючи уразливості, активний порушник може виконувати комбінацію атак, яка може привести до досягнення несанкціонованого доступу.

В якості основних можливих атак активного порушника виділені:

• Перебір пароля для доступу до управління обладнанням оператора або користувача;

• Організація проксінг або перенаправлення всього або частини трафіку будь-яким доступним способом;

• Виконання атаки MITM на ПРК і інші протоколи безпечної IP-телефонії;

• Атака на шифр - перебір ключа до перехопленому медіа трафіку;

• Установка закладки, модифікація програмного забезпечення (ПЗ) терміналу користувача;

• Установка додаткового обладнання на вузлі оператора зв'язку;

• Зміна налаштувань терміналу користувача для часткового відключення безпеки;

• Перехоплення авторизаційних даних для управління терміналом користувача за рахунок прослуховування трафіку управління шлюзом.

Атака перебір пароля до обладнання дозволяє отримати нелегітимного користувачеві контроль над атакується обладнанням для подальшої організації атаки несанкціонованого доступу. Складність атаки залежить від протоколу управління, на який виконується атака (telnet, ssh, snmp, web і т.д.), від довжини використовуваних паролів, обчислювальних ресурсів порушника, і додаткових обмежень і захисних механізмів, що атакується обладнання, а також від ширини каналу зв'язку між порушником і жертвою. Атака виконується з використанням спеціалізованого програмного забезпечення при наявності каналу зв'язку для віддаленого доступу до інтерфейсу управління обладнанням.

Атака "організація проксінг або перенаправлення трафіку" дозволяє порушнику частково або повністю пропускати через своє обладнання трафік легітимного кореспондента. Це може бути досягнуто за рахунок використання функції віддзеркалення портів на обладнанні оператора, за рахунок використання маршрутизації на основі політик (policy based routing), а також за рахунок інших механізмів, доступних на обладнанні оператора зв'язку з комутацією пакетів.

Атака на ПРК полягає в організації MITM і вироблення ключів по черзі з кожним з кореспондентів. Вона дозволяє порушнику ставати проміжним елементом між кореспондентами і прослуховувати або модифікувати

передану інформацію. При цьому небезпека і поширеність даної атаки найбільш активно відзначається в різних джерелах масової інформації.

Атака на шифр полягає в отриманні ключа шифрування при наявності зашифрованого повідомлення. Атака може виконуватися за допомогою спеціалізованого програмного забезпечення, що здійснює перебір пароля на підставі часткової інформації про переданих даних.

Установка закладки, модифікація програмного забезпечення терміналу користувача дозволяє порушнику отримувати контроль над обладнанням користувача та будь-якою інформацією, що проходить через термінал, а також виконувати відведення інформації на свій сервер з метою виконання атаки несанкціонованого доступу.

Установка додаткового обладнання на вузлі оператора зв'язку, дозволяє порушнику виконувати модифікацію даних, переданих між кореспондентами, без необхідності зміни маршрутизації на мережевому обладнанні оператора. Атака виконується за рахунок включення між обладнанням оператора і кореспондента обладнання порушника, або підключення цього обладнання в мережу передачі даних оператора.

Атака "зміна налаштувань терміналу користувача для зниження рівня безпеки" може виконуватися за рахунок зміни таблиці маршрутизації на терміналі користувача, часткового відключення механізмів безпеки, наприклад, зміна режиму роботи протоколу SRTP на аутентифікацію повідомлень без шифрування, модифікації даних телефонної книжки і т.д.

Атака "перехоплення авторизаційних даних користувача, що застосовуються для управління VoIP-терміналом", може бути виконана внутрішнім порушником, що знаходяться в одній підмережі з легітимним користувачем, і досягається шляхом перехоплення трафіку в момент авторизації користувача на VoIP терміналі за рахунок атаки на MAC-таблицю обладнання, або перенастроювання мережевого обладнання.

2.3 Приватні моделі порушників

При розробці моделі порушника введено допущення, що якщо суб'єкт атаки знаходиться в одній мережі з об'єктом атаки, то такий порушник є внутрішнім. В іншому випадку він є зовнішнім. Тоді проміжними цілями порушників з точки зору отримання несанкціонованого доступу є [21]:

ЦА) захоплення обладнання оператора зовнішнім порушником; ЦБ) захоплення терміналу користувача зовнішнім порушником; ЦВ) захоплення обладнання оператора внутрішнім порушником; ЦГ) захоплення терміналу користувача внутрішнім порушником. Кінцевою метою кожної атаки є НСД.

2.3.1 Зовнішній порушник

Розробка моделі починається з аналізу алгоритмів дій порушника по кожній з перерахованих цілей.

2.3.1.1 Захоплення обладнання оператора зовнішнім порушником

Розглянуто модель для зовнішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення обладнання оператора. Алгоритм дій порушника наведено на рис. 2.2.

Для початку атаки порушник повинен визначити, на який ресурс або який пристрій оператора почати виконувати атаку. Однією з можливостей отримати цю інформацію є використання команди tracert для визначення проміжних вузлів між порушником і жертвою. Відповідно – з великою ймовірністю ці вузли можуть брати участь в обміні пакетами між двома кореспондентами.

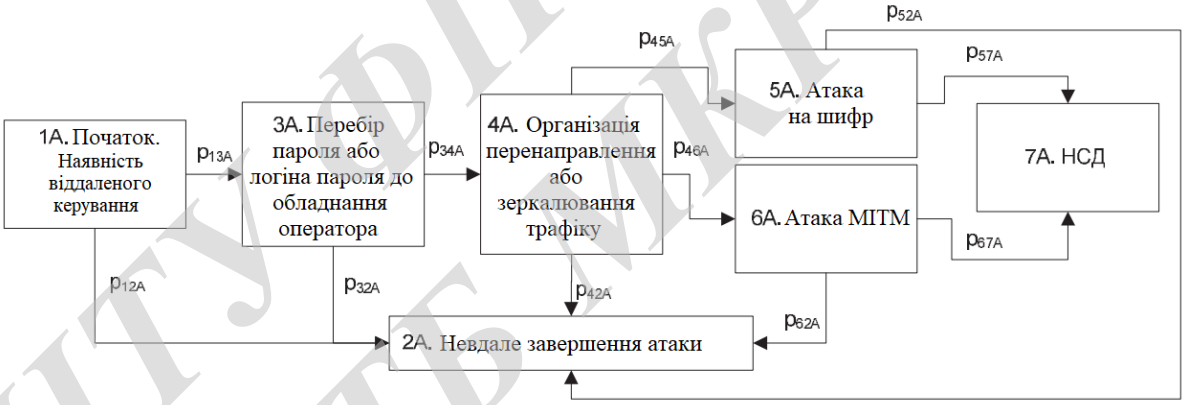


Рисунок 2.2 - Можливий алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником

Після вибору вузла порушник може спробувати захопити управління цим вузлом, виконуючи, наприклад, атаку перебір пароля. Однак - технічно віддалене управління може бути заборонено для порушника з використанням списків доступу ACL (Access Control List).

Імовірність p12 відображає подія, що віддалене управління з боку порушника відключено або у оператора встановлені ACL.

Імовірність p13 відображає подія, зворотне p12, що існує можливість віддаленого підключення до пристрою оператора.

Порушник вибирає доступний протокол (telnet, SNMP, ssh, http / https або ін.) Віддаленого управління, на який буде виконувати атаку перебором пароля. Імовірність успішного перебору пароля за обмежений час визначається, як:

$$p_{34A} = F\ (l, D, T, C), \tag{2.1}$$

де l - довжина логіну / пароля;

T - час, протягом якого потрібно виконати перебір;

D - додаткові обмеження протоколу, що утрудняють виконання перебору пароля, а так само технічні можливості порушника;

C - швидкість каналу зв'язку, за яким виконується перебір.

Імовірність p34A відображає подія, що перебір пароля виконаний успішно і порушник отримав доступ на обладнання оператора. Імовірність p32 відображає подія, що перебір пароля за обмежений час закінчився не успішно.

У разі успішного захоплення віддаленого управління, порушник може досягти НСД двома шляхами: виконати перебір пароля до переданому медіа трафіку і прослуховувати дані, або виконати атаку на механізм розподілу ключів і дешифрувати трафік з використанням отриманого ключового матеріалу. Однак - успішне виконання цих двох атак може не привести до позитивного результату по досягненню НСД, якщо не існує можливості виконати атаку MITM на медіа трафік, створивши правила на обладнанні оператора, які дозволять порушнику пропускати трафік користувача через своє обладнання. З цієї причини - подія "атака на медіа трафік" в моделі порушника перенесено раніше, ніж "перебір ключа медіа трафіку", або "атака на механізм розподілу ключів".

Імовірність успішної атаки на медіа трафік (MITM, організація проксінг) можна визначити за формулою:

$$1\text{-}p_{42A} = \begin{cases} 1, \text{якщо існує технічна можливість на обладнанні оператора} \\ \text{створити правило для перенаправлення трафіку користувача} \\ \text{в сторону порушника для виконання цілей "проксінг" MITM} \\ 0, \text{якщо не існує такої технічної можливості} \end{cases}. \tag{2.2}$$

Під атакою розуміється зміна маршруту передачі пакетів мультимедійних файлів, щоб вони проходили через обладнання порушника. У разі успішного проведення атаки порушник намагається виконати одну з двох можливих атак.

• перебір ключа медіа трафіку;

• атака на механізм розподілу ключів. При цьому ймовірності відображають:

p_{45A} - ймовірність, що порушник почав виконувати перебір пароля до медіа трафіку.

p_{46A} - ймовірність, що порушник почав атаку на механізм розподілу ключів VoIP.

Імовірність p_{57} означає успішну атаку по перебору пароля. В цьому випадку - порушнику ставати доступно прослуховування медіа трафіку одного конкретного розмови, а також модифікації даних при наявності проксінг і швидкого дешифрування ключа.

Імовірність p_{52} відображає неуспішне закінчення атаки по перебору пароля за обмежений час. Перехоплені дані можуть зберігатися у порушника скільки завгодно довго, проте актуальність перехоплених даних може застарівати згодом. Так розшифровані через 100 років переговори можуть не принести ніякої користі порушнику, так як за цей час дані втратять актуальності. TNAR_AKT - час, протягом якого дані є актуальними - залежить від характеру даних. TNAR_SRTP - час, необхідний на перебір пароля, залежить від технічних потужностей порушника - NarTH, що застосовуються для захисту мультимедійних файлів криптографічних примітивів і криптоалгоритмів - NarK, довжини ключа - NarL, а також від ускладнюючих елементів (застосування не започатковано вектора, додаткових лічильників і т.д.) - NarD.

$$p_{57A} = f\,(T_{NAR\_AKT}, T_{NAR\_SRTP}) = f\,(T_{NAR\_AKT}, Nar_{TH}, Nar_K, Nar_L, Nar_D); \quad (2.3)$$

$$p_{52A} = 1\ p_{57A}\ . \quad (2.4)$$

Імовірність p_{67} визначає успішну атаку на механізм розподілу ключів. Під атакою розуміється вторгнення порушника в середину каналу зв'язку в момент обміну ключами між кореспондентами. Це дозволяє порушнику виробити два ключа - один для роботи з першим кореспондентом і другий для роботи з другим кореспондентом. Тим самим, під час розмови двох кореспондентів порушник виконує шифрування і дешифрування мультимедійних файлів з використанням власних джерел. Імовірність атаки залежить від наявності у порушника технічних і програмних засобів для проведення MITM на протокол розподілу ключів.

Слід зазначити, що для проведення даної атаки потрібна розробка спеціалізованого програмного забезпечення, але не потрібні великі обчислювальні потужності.

Імовірність p_{62} відображає неуспішне виконання атаки і може бути визначена, як:

$$p_{62A} = 1\text{-}p6_{7A} \quad (2.5)$$

Для аналізу алгоритму використовується математичний апарат імовірнісних графів [27], який дозволяє отримати для досліджуваного алгоритму оцінки середнього часу виконання і ймовірність успішного завершення.

На рис. 2.3 представлений імовірнісний граф, відповідний наведеним раніше алгоритму. Імовірнісний граф використовується для отримання виробляє функції, відповідної переходу системи з початкового стану в кінцеве.

Кожній гілки графа відповідає виробляє функція виду:

$$H_{zy} = p_{zy}x^{Tzy}, \quad (2.6)$$

де p_{zy} - ймовірність переходу в стан y з стані z,

T_{zy} - час, необхідний для переходу зі стану z в стан y.

Використовуючи можливий алгоритм дій порушника, складений імовірнісний граф, представлений на рис. 2.3.

За графу виділена гілка, відповідна успішному виконанню атаки НСД і складена виробляє функція H (x) цієї гілки.

Для графа відповідно до методики, наведеної в [22], представлені $P_{НСД}$ = H (x = 1):

$$Pнсд_{ЦА} = p_{13A}\, p_{34A}\, (p_{45A}p_{57A} + p_{46A}p_{67A}), \quad (2.7)$$

де p_{ijA} - ймовірність переходу з вершини i графа в вершину j.

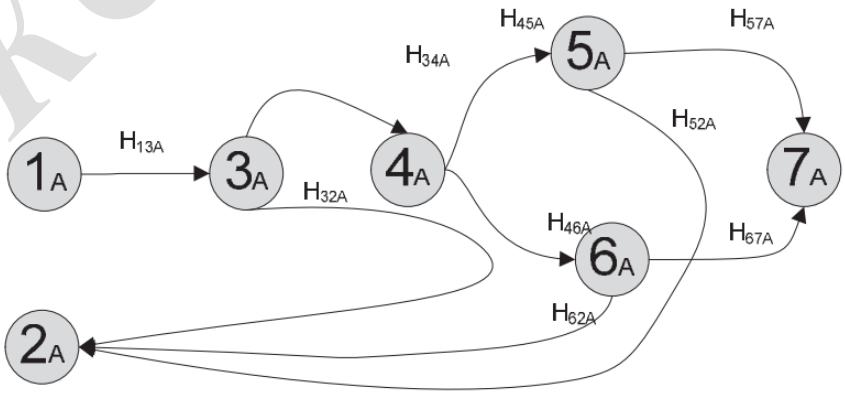


Рисунок 2.3 - Імовірнісний граф - захоплення обладнання оператора зовнішнім порушником

2.3.1.2 Захоплення терміналу користувача зовнішнім порушником

Розглянуто модель для зовнішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення терміналу користувача. Алгоритм дій порушника наведено на рис. 2.4.

Розглянуто детальніше атаки, які може зробити порушник, в залежності від використання у одного з кореспондентів шлюзу або персонального комп'ютера зі спеціалізованим програмним забезпеченням.

При використанні шлюзу найбільш вірогідною є атака з проксінг всього трафіку через обладнання порушника. Атака виконується за схемою, зазначеної на рис. 2.5, де IP1, IP2 - шлюзи користувачів, а Sн - сервер порушника зі спеціалізованим програмним забезпеченням.

Для проведення цієї атаки порушника потрібно в першу чергу захопити управління VoIP терміналом користувача і виконати його перенастроювання. Наприклад - якщо у кореспондента в режимі точка-точка в телефонній книжці шлюзу введені поєднання номер - IP-адреса, то порушник може підмінити IP - адреса кореспондента Б в записнику кореспондента А на свій, тим самим дзвінки з телефону кореспондента А будуть приходити на Sн. Далі - сервер порушника виконує протоколи безпеки між собою і кореспондентом Б від імені кореспондента А. Протоколи безпеки теж виконуються між кореспондентами Б і сервером порушника. В результаті -
порушник отримує доступ до всієї інформації, що передається від кореспондента А до кореспондента Б, у відкритому вигляді і при необхідності може не тільки прослуховувати, але і змінювати дані, що передаються між кореспондентами. Перенаправлення трафіку від кореспондента А на Sн можна здійснювати не тільки за рахунок підміни записи в адресній книзі, а й за рахунок зміни налаштувань на шлюзі кореспондента А, встановивши адресу свого Sн в якості проксі-сервера або основного сервера IP-телефонії.

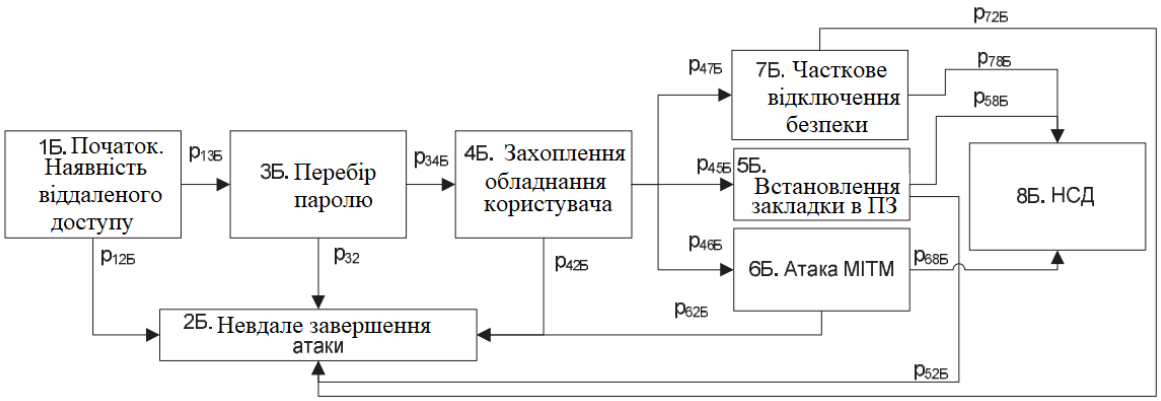


Рисунок 2.4 - Можливий алгоритм дій при захоплення терміналу користувача зовнішнім порушником

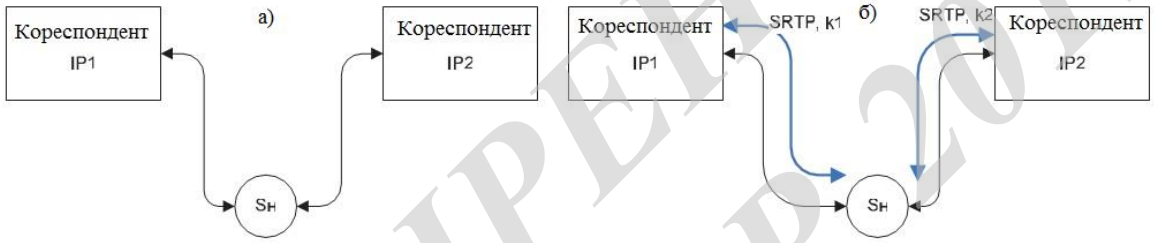


Рисунок 2.5 - Атака з проксінг а) виконання ПРК, б) встановлений захищений мовний канал

При використанні комп'ютера з встановленим програмним шлюзом IP-телефонії найбільш реалізованими є атаки:

- атака з проксінг всього медіарафіка кореспондентів через Sн;
- впровадження програми-шпигуна на комп'ютер.

Перший вид атаки був описаний раніше. Атака з впровадженням програми-шпигуна полягає в установці на термінал користувача програмного забезпечення, яке відправляє голосові дані у відкритому вигляді з терміналу або передає всі вихідні і вхідні пакети з мережевого інтерфейсу терміналу користувача на S н для подальшої обробки. Тоді для доступу до інформації, що передається порушнику може знадобитися вимкнути застосовуються на терміналі користувача А протоколи безпеки IP-телефонії, або, як мінімум, змінити режим роботи SRTP, вимкнувши шифрування переданих мультимедійних файлів.

Як правило, IP-телефони і шлюзи мають можливість віддаленого управління, яка використовується самими користувачами для їх налаштування. Обчислювальні пристрої також можуть мати дистанційне

керування, організоване внутрішніми засобами застосовуваної операційної системи, або з використанням додаткового програмного забезпечення. Однак, віддалене управління може бути також відключено користувачем, або можливості віддаленого управління можуть бути обмежені за рахунок застосування списків доступу.

Для успішного виконання атаки порушник повинен захопити віддалене управління призначеним для користувача терміналом. В першу чергу - успіх атаки залежить від багатьох факторів. Імовірність успішного проведення цього етапу атаки розглядається, як:

$$p_{34Б}=\begin{cases}1, \text{якщо у користувача терміналу включено віддалене управління} \\ \quad \text{і немає настояних списків доступу на всі видалені протоколи} \\ 0, \text{якщо у користувача терміналу включено віддалене управління.} \\ \quad \text{і є настояні списки доступу на всі видалені протоколи} \\ 0, \text{якщо у користувача терміналу вимкнено віддалене управління}\end{cases} \quad (2.8)$$

При наявності віддаленого управління, порушнику для проведення атаки потрібно підібрати пароль або пару логін-пароль для авторизації на терміналі користувача [28]. Передбачається, що IP адреса жертви відомий порушнику заздалегідь. Підбір пароля або логіна-пароля залежить від протоколу віддаленого управління, на який виконується атака. Імовірність успішного перебору пароля має сенс оцінювати за кінцевий інтервал часу T, тому що ймовірність успішного перебору пароля за нескінченний час буде дорівнює 1.

Імовірність успішного перебору пароля можна визначити як:

$$p_{45Б}=F(l, D, T, C), \quad (2.9)$$

де l - довжина логіна-пароля;

T - час, протягом якого потрібно завершити перебір;

D - додаткові обмеження протоколу, що утрудняють виконання перебору пароля, а так само технічні можливості порушника;

C - швидкість каналу зв'язку, за яким виконується перебір.

Після успішного перебору пароля і отримання доступу до терміналу користувача, порушник з певною ймовірністю може вибрати один з двох можливих шляхів:

- установка закладки, модифікація ПО терміналу;
- зміна налаштувань терміналу користувача;
- MITM для всіх протоколів IP-телефонії.

Можливість вибору однієї з двох атак визначається технічною оснащеністю порушника, а також наявністю у нього спеціалізованих інструментів і засобів.

Сенс першої атаки полягає в захопленні голосової інформації в обхід протоколів IP-телефонії, або в виключенні протоколів безпеки IP- телефонії, або зміні режимів роботи протоколів безпеки IP-телефонії, щоб можна було виконувати прослуховування.

Сенс другої і третьої атаки полягає в зміні налаштувань користувача терміналу для реалізації атаки MITM, при якій всі дані протоколів безпеки проходять через порушника, що дозволяє йому контролювати передані голосові пакети, а також при необхідності виконувати модифікацію переданих даних. Фактично, при даній атаці порушник виконує з'єднання по черзі з кожним з кореспондентів, використовуючи протоколи забезпечення безпеки IP-телефонії, реалізуючи схему, представлену на рис. 2.6.

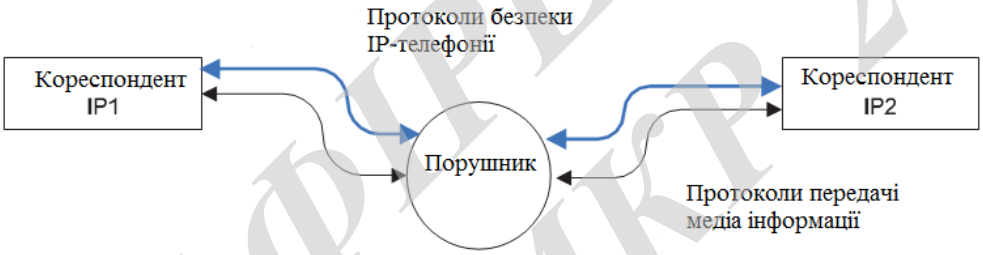


Рисунок 2.6 - Реалізація атаки MITM для всіх протоколів забезпечення безпеки VoIP.

Вибравши одну з атак, порушник спробує виконати її для отримання несанкціонованого доступу до інформації, що передається. Однак існує ймовірність неуспішного виконання обраної атаки, від якої потерпають можливостями p_{72} і p_{62} відповідно. Наприклад - атака "зміна налаштувань терміналу користувача" може скінчитися не успішно, якщо користувач помітить змінені настройки і відновить свої настройки, змінивши паролі доступу до терміналу або відключивши вилучене керування.

Використовуючи можливі алгоритми дій порушника, складений імовірнісний граф, представлений на рис. 2.7.

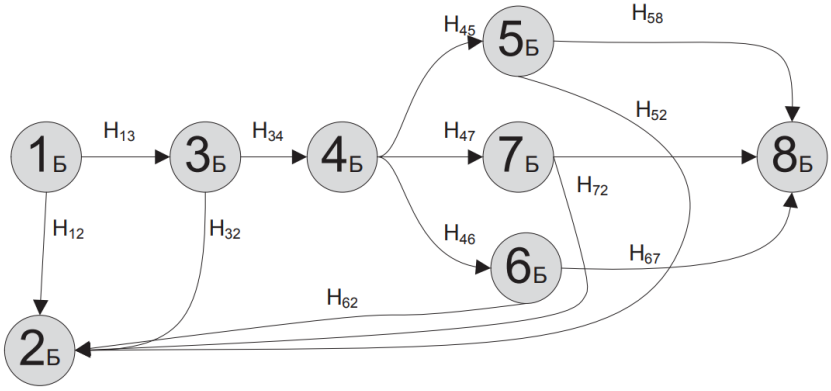


Рисунок 2.7 - Імовірнісний граф захоплення терміналу користувача зовнішнім порушником

З графа виділена гілка, відповідна успішному виконанню атаки НСД, і складена виробляє функція H (x) цієї гілки.

Для графа відповідно до методики, наведеної в [27], представлені $P_{НСД} = H(x=1)$:

$$P_{нсдЦБ}=p_{13Б}p_{34Б}(p_{45Б}p_{58Б}+p_{46Б}p_{68Б}+p_{47Б}p_{78Б}), \quad (2.10)$$

где $p_{ijБ}$ – ймовірність переходу із i-ї в j-у вершину графа.

2.3.2 Внутрішній порушник

2.3.2.1 Захоплення обладнання оператора внутрішнім порушником

Розглянуто модель внутрішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення обладнання оператора.

У порівнянні із зовнішнім порушником, внутрішній щодо оператора порушник має низку переваг. Він спочатку має певний рівень доступу на обладнання оператора зв'язку, а також може мати можливість установки і підключення додаткового обладнання до існуючого обладнання на мережі оператора.

Якщо порушник не має достатнього рівня доступу на обладнання оператора, він може спробувати отримати доступ, виконуючи атаку перебору паролів для отримання більш високого рівня.

Алгоритм дій порушника наведено на рис. 2.8.

p_{18B} характеризує ймовірність, що у внутрішнього порушника спочатку є доступ достатнього рівня для проведення подальших дій для досягнення несанкціонованого доступу.

Імовірність p_{18B} може бути визначена, як:

$$p_{18B}=\begin{cases}1, \text{якщо порушник має достатній рівень доступу;}\\ 0, \text{якщо порушник не має достатній рівень доступу.}\end{cases} \quad (2.11)$$

p_{19B} відображає ймовірність події, що порушнику вдалося підключити своє додаткове обладнання в мережі оператора на вузол, через який проходить медіа трафік жертви.

$$p_{19B}=\begin{cases}1, \text{якщо порушник зміг встановити додаткове обладнання на вузлі оператора;}\\ 0, \text{якщо порушник не зміг встановити додаткове обладнання на вузлі оператора.}\end{cases} \quad (2.12)$$

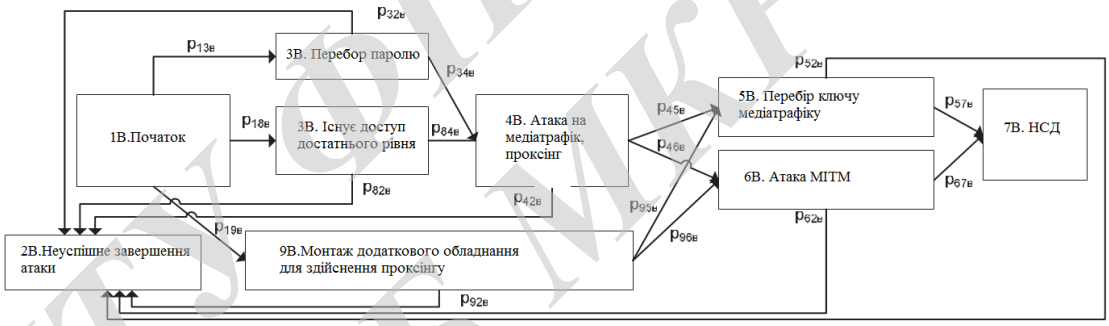


Рисунок 2.8 - Можливий алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником

Встановлюється обладнання спочатку повинно мати функціонал модифікації або віддзеркалення пакетів. З цього кроку порушник може вибирати один з двох шляхів для подальшого проведення атаки. Вибір залежить від технічних можливостей встановленого обладнання. Однак, навіть при установці устаткування порушника є певна ймовірність, що атака може бути проведена не успішно. Наприклад - це може статися в тому випадку, якщо клієнти почнуть застосовувати додаткові механізми для відстеження вторгнення або додаткові протоколи, використання яких може бути не врахована в обладнанні порушника.

Використовуючи можливі алгоритми дій порушника, складений імовірнісний граф, представлений на рис. 2.9.

У графі виділена гілка, відповідна успішному виконанню атаки НСД і складена виробляє функція H(x) цієї гілки. Для графа відповідно до методики, наведеної в [27], представлені $P_{НСД.}$

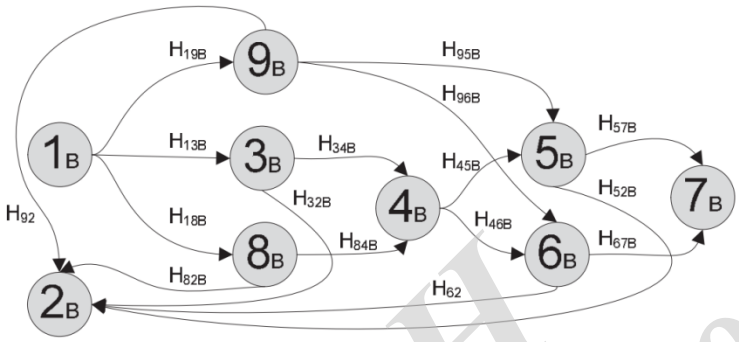


Рисунок 2.9 - Імовірнісний граф - Захоплення обладнання оператора внутрішнім порушником

$$P_{нсдЦВ}=((p_{13B}p_{34B}+p_{18B}p_{84B})p_{45B}+p_{19B}p_{95B})p_{57B}+$$
$$((p_{13B}p_{34B}+p_{18B}p_{84B})p_{46B}+p_{19B}p_{96B})p_{67B}\ , \qquad (2.13)$$

де p_{ijX} – ймовірність переходу з вершини і в вершину j графа. Тоді ймовірність захисту від атаки НСД матиме вигляд:

$$P_{зах\_нсд\_B}=1-P_{нсдЦВ}=$$
$$=1-((p_{13B}p_{34B}+p_{18B}p_{84B})p_{45B}+p_{19B}p_{95B})p_{57}+((p_{13B}p_{34B}+p_{18B}p_{84B})p_{46B}+p_{19B}p_{96B})p_{67B}, \qquad (2.14)$$

де p_{13B} – ймовірність вибору атаки перебір пароля для доступу до обладнання оператора;

p_{18B} – ймовірність наявності доступу достатнього рівня на обладнання оператора;

p_{19B} – ймовірність наявності у порушника можливості установки додаткового обладнання для виконання атаки;

p_{34B} – ймовірність успішного завершення атаки перебір пароля для доступу до обладнання оператора;

p_{45B} – ймовірність вибору атаки "злом шифру";

p_{46B} – ймовірність вибору "атака на механізм розподілу ключів";

p_{57B} – ймовірність успішного завершення атаки "злом шифру";

p_{67B} – ймовірність успішного завершення атаки "атака на механізм розподілу ключів

p_{95B} – ймовірність вибору атаки "злом шифру";

p_{96B} – ймовірність вибору "атака на механізм розподілу ключів".

2.3.2.2 Захоплення терміналу користувача внутрішнім порушником

Розглянуто модель для внутрішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення терміналу користувача. Алгоритм дій порушника наведено на рис. 2.10.

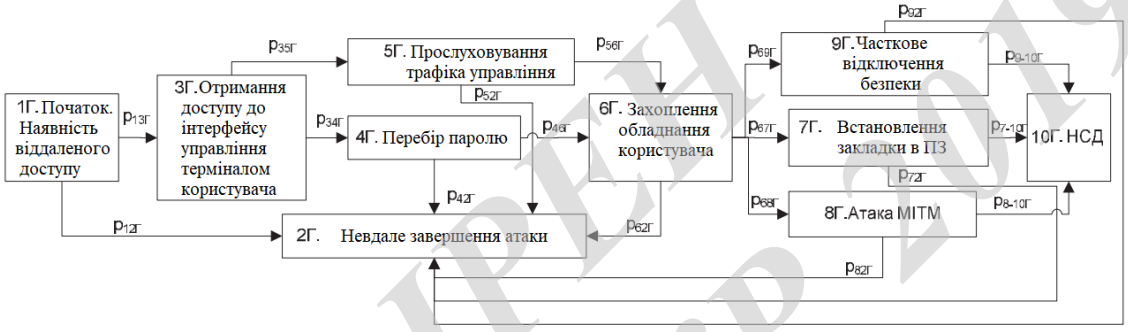


Рисунок 2.10 - Можливий алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником

Використовуючи можливий алгоритм дій порушника, складений імовірнісний граф, представлений на рис. 2.11. З графа виділена гілка, відповідна успішному виконанню атаки НСД, і складена виробляє функція H (x) цієї гілки. Для графа відповідно до методики [27] представлена ймовірність успішного завершення атаки НСД - $P_{НСД}$:

$$P_{нсдЦГ}=p_{13Г}(p_{34Г}p_{46Г}+p_{35Г}p_{56Г})(p_{67Г}p_{7\text{-}10Г}+p_{68Г}p_{8\text{-}10Г}+p_{69Г}p_{9\text{-}10Г}), \quad (2.15)$$

де $p_{ijГ}$ – ймовірність переходу з вершини і графа в вершину j.

Імовірність захисту від атаки матиме вигляд:

$$P_{зах\_нсд\_Г}=1\text{-}P_{нсдЦГ}=1\text{-}p_{13}(p_{34}p_{46}+p_{35}p_{56})(p_{67}p_{7\text{-}10}+p_{68}p_{8\text{-}10}+p_{69}p_{9\text{-}10}), \quad (2.16)$$

де $p_{13Г}$ - ймовірність наявності віддаленого підключення;

$p_{34Г}$ - ймовірність вибору атаки "перебору пароля до обладнання користувача";

$p_{46Г}$ - ймовірність успішного перебору пароля до обладнання користувача за обмежений час;

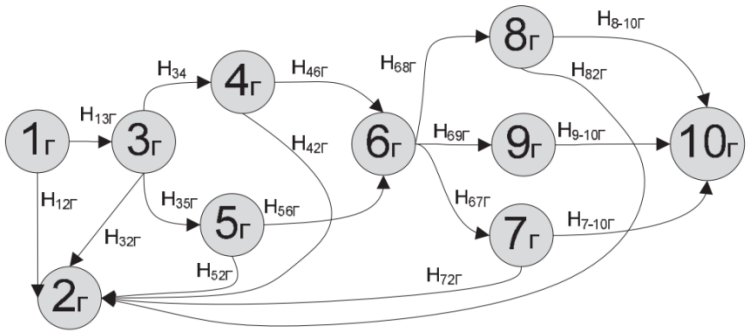


Рисунок 2.11 - Імовірнісний граф - захоплення терміналу користувача внутрішнім порушником

$p_{35Г}$ – ймовірність вибору атаки "отримання пароля до обладнання користувача за рахунок прослуховування трафіку користувача";

$p_{56Г}$ – ймовірність успішного завершення атаки "перехоплення пароля до обладнання користувача за рахунок прослуховування трафіку управління";

$p_{68Г}$ – ймовірність вибору атаки MITM для всіх протоколів VoIP;

$p_{8\text{-}10Г}$ – ймовірність успішного завершення атаки MITM для всіх протоколів VoIP;

$p_{67Г}$ – ймовірність вибору атаки "установка закладки на терміналі користувача";

$p_{7\text{-}10Г}$ – ймовірність успішного завершення атаки "установка закладки на терміналі користувача або відключення безпеки"

$p_{6\text{-}9Г}$ – ймовірність вибору атаки "повне або часткове відключення безпеки";

$p_{9\text{-}10Г}$ – ймовірність успішного завершення атаки "повне або часткове відключення безпеки".

Значення багатьох ймовірностей, що входять в формулу, вимагають експертної оцінки і не можуть бути обчислені. Також значення цих ймовірностей залежать від порушника, його можливостей, а також додаткових обставин.

2.4 Оцінка ймовірності успішного завершення атаки

Для кожного з розглянутих графів відповідно до методики, наведеної в [27], наведені $P_{НСД}$:

$$P_{нсдЦА} = p_{13А}\, p_{34А}(p_{45А}p_{57А} + p_{46А}p_{67А}), \quad (2.17)$$

$$P_{нсдЦБ} = p_{13Б}p_{34Б}(p_{45Б}p_{58Б} + p_{46Б}p_{68Б} + p_{47Б}p_{78Б}), \quad (2.18)$$

$$P_{нсдЦВ} = ((p_{13В}p_{34В} + p_{18В}p_{84В})p_{45В} + p_{19В}p_{95В})p_{57В} + \\ + ((p_{13В}p_{34В} + p_{18В}p_{84В})p_{46В} + p_{19В}p_{96В})p_{67В}\ , \quad (2.19)$$

$$P_{нсдЦГ} = p_{13Г}(p_{34Г}p_{46Г} + p_{35Г}p_{56Г})(p_{67Г}p_{7\text{-}10Г} + p_{68Г}p_{8\text{-}10Г} + p_{69Г}p_{9\text{-}10Г}), \quad (2.20)$$

де p_{ijX} – ймовірність переходу з вершини і в вершину j відповідного графа.

$$P_{нсд} = max\ \{ P_{нсдЦА}, P_{нсдЦБ}\ , P_{нсдЦВ}, P_{нсдЦГ} \}. \quad (2.21)$$

Очевидно, в разі встановлення з'єднання в сценарії кореспондент-кореспондент без сервера і при відсутності попередньо розподіленого ключового матеріалу, сам користувач є найбільш зацікавленою особою для підвищення безпеки і зниження $P_{НСД}$. При цьому користувач може застосовувати VoIP термінал, що підтримує функцію відключення віддаленого управління, що призведе до $p_{13Б} = 0$, $p_{13Г} = 0$, і як наслідок, $P_{НСДЦБ} = 0$, $P_{НСДЦГ} = 0$.

Однак, користувач не може впливати на ймовірності pij_A, pij_B. Залежно від проміжних цілей порушника виділяється кілька приватних моделей порушників, представлених в табл. 2.1.

Слід зауважити, що $p_{57А}$, $p_{57В}$ залежать від застосовуваного алгоритму шифрування. Існуючі рекомендації SRTP передбачають застосування алгоритму AES с ключем 128 або 256 біт. Злом такого алгоритму є вкрай малоймовірним [28]. Тому найбільш вірогідним буде вибір атаки MITM на ПРК з боку порушника. Отже, можна ввести допущення, що ймовірність вибору атаки на шифр $p_{45А}=0$, $p_{45В}=0$, а ймовірність вибору атаки MITM $p_{46А}=1$, $p_{46В}=1$.

Таблиця 2.1 - Ймовірності атак в залежності від цілей порушника

Позначення і визначення	Можл	Цілі порушника

ймовірності		B1) Атака внутрішнього порушника через захоплення обладнання оператора за рахунок перебору пароля і організація MITM	B2) Атака внутрішнього порушника при наявності у нього доступу на обладнання шляхом організації MITM	B3) Атака внутрішнього порушника через установку додаткового обладнання на вузлі оператора шляхом організації MITM	A4) Атака зовнішнього порушника через захоплення обладнання оператора за рахунок перебору
p_{13B} – Імовірність вибору нападу "порушення пароля для доступу до обладнання оператора "	0..1	1	0	0	-
p_{18B} – Імовірність наявності достатнього доступу до обладнання оператора	0..1- p_{13B}	0	1	0	-
p_{19B} – можливість зловмисника Встановити Додаткове обладнання на вузол оператора для Здійснення нападу	0..1- p_{18B}- p_{13B}	0	0	1	-
p_{34A},p_{34B} – Імовірність успішного завершення атаки шляхом розоряє пароль для контролю обладнання оператора	0..1	0..1	-	-	0..1
p_{84B} – можливість порушника, використовуючи достатній доступ до обладнання оператора	0..1	-	0..1	-	-
p_{46A}, p_{46B} – Імовірність вибору "MITM атак на ФРК та інші безпечні протоколи IP телефонії"	0..1- p_{45A} 0..1- p_{45B}	1	1	-	1
p_{67A},p_{67B} – Імовірність успішного завершення "MITM напад на ФРК та інші безпечні протоколи IP телефонії"	0..1	0..1	0..1	0..1	0..1
p_{96B} – Імовірність вибору "MITM атак на ФРК та інші безпечні протоколи IP телефонії"	0..1- p_{95B}	-	-	1	-
p_{13A} – Імовірність можливості віддалено підключатися до обладнання оператора	0 чи 1	-	-	-	1

Тоді ймовірність успішної атаки НСД матиме вигляд:

$$P_{нсд} = max\ \{ P_{нсдЦА}, P_{нсдЦВ} \}, \quad (2.22)$$

$$P_{нсдЦА}=p_{13A}p_{34A}p_{46A}p_{67A}\ , \quad (2.23)$$

$$P_{нсдЦВ}=((p_{13B}p_{34B}+p_{18B}p_{84B})p_{46B}+p_{19B}p_{96B})p_{67B}\ , \quad (2.24)$$

Залежно від проміжних цілей і можливостей також виділяється кілька порушників (В1, В2, В3, А4), представлених в табл. 2.1.

Підставивши значення p_{ijX} з таблиці в формули 2.23, 2.24 отримуємо:

$$P_{нсдВ1}=p_{34B}p_{67B}\,, \tag{2.25}$$

$$P_{нсдВ2}=p_{84B}p_{67B}\,, \tag{2.26}$$

$$P_{нсдВ3}=p_{67B}\,, \tag{2.27}$$

$$P_{нсдА4}=p_{34A}p_{67A}\,, \tag{2.28}$$

$$P_{НСД}=max\{P_{нсдВ1}, P_{нсдВ2}, P_{нсдВ3}, P_{нсдА4}\}. \tag{2.29}$$

Очевидно, що $P_{нсдВ3}$ більше або дорівнює $P_{нсдВ1}$, $P_{нсдВ2}$, $P_{нсдА4}$. Тому, $P_{НСД}$ буде визначатися за величиною p_{67B}, яка буде відповідати атаці НСД внутрішнього порушника на вузлі оператора зв'язку за допомогою установки додаткового обладнання для організації MITM. Тому, доцільно скоротити p_{67B}, забезпечуючи захист від порушника, націленого на MITM. Графік залежності $P_{НСД}$ для моделі захоплення обладнання оператора зовнішнім порушником наведено на рис. 2.12.

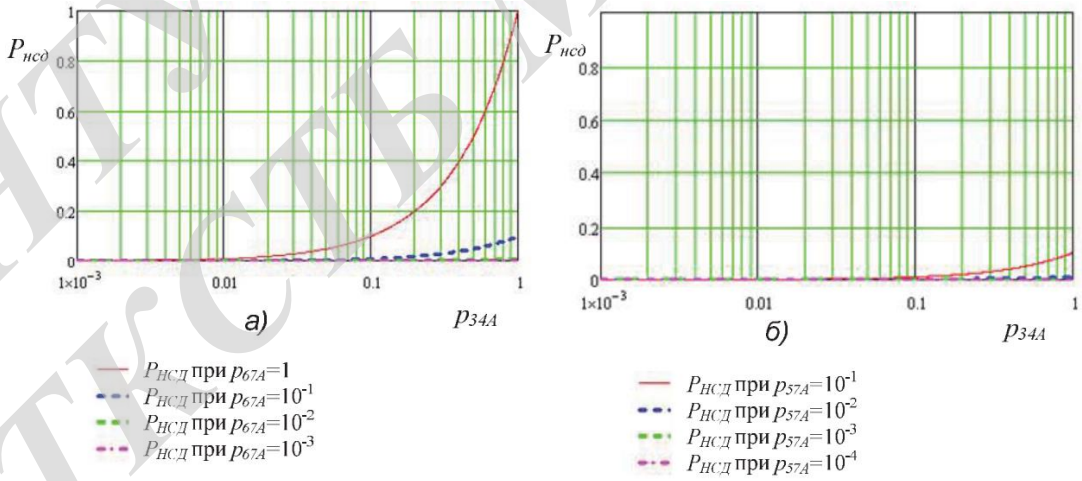


Рисунок 2.12 – Залежність $P_{НСД}$ для моделі - захоплення обладнання оператора зовнішнім порушником а) при виборі MITM б) при виборі атаки на шифр

2.5 Висновки до розділу 2

Наведено визначення порушника і опис терміналу користувача. Показана сукупність атак, які може виконувати порушник для досягнення

несанкціонованого доступу. Представлено математичну модель активного порушника для захищеної IP-телефонії, що враховує можливості цього порушника реалізувати атаку MITM на ПРК і інші атаки. Модель дозволяє розрахувати ймовірність успішної атаки, націленої на НСД, в залежності від значень ймовірностей проміжних атак. Наведено приватні моделі порушників в залежності від обраних цілей, можливостей і місця розташування порушника.

Для боротьби з порушником, які поставили за мету захопити управління обладнанням користувача, необхідно виконувати всі рекомендації щодо забезпечення безпеки під час налаштування обладнання, а саме, блокувати віддалене управління з нелегітимних і інших мереж, або відключати віддалене управління.

Наведено оцінку ймовірності вибору кожним з приватних порушників певних проміжних цілей при реалізації атаки. Показані можливі дії користувача для захисту від атак, а також визначена найбільш небезпечна для користувача атака MITM на протокол забезпечення безпеки IP - телефонії, яка також є найкращою для порушника.

Показано, що особливу небезпеку становить зовнішній і внутрішній порушники, які виконують атаку на обладнання оператора. Представлена імовірнісна модель такого порушника. Показано, що найбільш небезпечною є атака MITM на протоколи розподілу ключового матеріалу.

3 РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ВДОСКОНАЛЕННЯ ПРОТОКОЛІВ РОЗПОДІЛУ КЛЮЧІВ

Для дослідження ймовірносно-часових характеристик необхідно розглянути протоколи розподілу ключів захищеної IP-телефонії, що відповідають вимогам до ПРК, описаним в першому розділі:

– К1. Підтримка топологій клієнт-сервер і клієнт-клієнт;

– К2. Самодостатність (функціонування без застосування додаткових протоколів між кореспондентами для реалізації функції розподілу ключів);

– К3. Робота без передачі ключа у відкритому вигляді по каналу зв'язку;

– К4. Наявність механізму виявлення MITM без заздалегідь розподіленого ключового матеріалу між кореспондентами, а також без використання сертифікатів;

– К5. Використання TCP / UDP портів, що застосовуються для IP-телефонії (SIP / RTP), або TCP / UDP портів, використання яких узгоджено в результаті встановлення з'єднання;

Якщо вимога виконується, K_i=1. В інакше K_i=0.

Порівняння протоколів приведено в табл. 3.1.

Таблиця 3.1 - Оцінка ПРК на відповідність вимогам

Опис вимоги до ПРК	Протоколи			
	DTLS	ZRTP	SDES	MIKEY
K_1	1	1	0	1
K_2	1	1	0	0
K_3	1	1	0	1
K_4	0	1	0	0
K_5	1	1	1	1
$Q_{ПРК}$	4	5	1	3

Оцінка кожного з протоколів проводиться відповідно до функції $Q_{ПРК}$:

$$Q_{ПРК} = \sum_{i=1}^{5} K_i \, . \qquad (3.1)$$

Протокол DTLS не відповідає четвертому вимогу, представленому в табл. 3.1, так як розроблявся для роботи в топології клієнт - сервер і використовує встановлені сертифікати для захисту від MITM у обох кореспондентів. Тому для DTLS $K_4 = 0$.

На відміну від інших протокол ZRTP має вбудований механізм SAS (Short Authentication String) для захисту від MITM. Тому для ZRTP $К_4 = 1$. Для SDES і MIKEY $К_4 = 0$.

Протокол MIKEY не задовольняє другій вимозі з табл. 3.1, так як повідомлення протоколу можуть передаватися або в SIP/SDP-повідомлення, або поверх RTSP (Real Time Streaming Protocol), але в останньому випадку кореспонденти повинні додатково підтримувати протокол RTSP. Тому $К_2 = 0$ для MIKEY.

П'ята вимога при роботі поверх RTSP протоколу не виконується, але при цьому виконується друга вимога. При роботі MIKEY поверх в SIP/SDP-повідомлення П'ята вимога виконується, але не виконується друга вимога. Так як при оцінці QПРК використовується $К_2 = 0$, то $К_1 = 1$ для MIKEY.

Протокол SDES не задовольняє першому і третьому вимогу ($К_1 = 0$ і $К_3 = 0$), так як ключ передається між кореспондентами в явному вигляді в повідомленнях SDP і вимагає їх додаткового захисту. Для захисту як правило використовується додатковий протокол SIPS. Однак, при з'єднанні клієнт клієнт, коли у кореспондентів немає заздалегідь розподіленого ключового матеріалу, SIPS з'єднання з захистом від MITM організувати неможливо. Протокол SDES не задовольняє другій вимозі, так як для передачі даних протоколу SDES використовуються повідомлення SIP/SDP. Відповідно $К_2 = 0$ для SDES.

Виходячи з табл. 3.1, в більшій мірі наведеним вимогам відповідають протоколи ZRTP і DTLS, що мають найбільше значення QПРК.

Оцінка ВВХ характеристик виконується для цих протоколів.

Результати проведених досліджень показують, що відомі протоколи розподілу ключів необхідно вдосконалювати в двох напрямках [26]:

1) підвищення безпеки;

2) поліпшення ВВХ характеристик протоколів.

У розділі 2 показано, що найбільш небезпечною атакою є атака MITM на протокол розподілу ключів. Завдання формування ключів в умовах вторгнення порушника в середину каналу зв'язку є актуальною і її вирішення присвячений ряд наукових робіт [27]. Особливістю даних робіт є те, що для формування ключів між кореспондентами використовується ефект незалежності випадкових процесів в різних точках середовища передачі сигналу. У протоколах формування ключів для IP-телефонії обмін повідомленнями реалізується на мережевому рівні і ефекти випадкових процесів в середовищі передачі даних однакові у всіх точках на трасі передачі пакетів, тому запропоновані підходи вкрай важко використовувати для розподілу ключів в IP-телефонії. Проводяться дослідження щодо підвищення безпеки протоколів

[29], однак спільністю даних робіт є необхідність наявності загального секрету між кореспондентами. Однак, ця умова не завжди може бути виконана.

Одним із шляхів підвищення безпеки протоколу є зниження ймовірності вторгнення порушника в протокол вироблення ключового матеріалу за рахунок використання декількох незалежних каналів зв'язку. Таким чином, використовувані в протоколі канали зв'язку повинні відповідати вимогу - не мати спільних точок, контролюючи які, порушник може одночасно атакувати використовувані канали.

В даному розділі проводиться дослідження ймовірності, що в обраному напрямку знайдеться хоча б два незалежних маршруту передачі даних, а також оцінка ймовірностей виявлення атаки при використанні декількох маршрутів одночасно, успішного вторгнення порушника в канали зв'язку, що використовуються під час виконання протоколу, а також успішного розподілу загального ключа . Пропонуються методи підвищення безпеки, засновані на використанні декількох каналів зв'язку одночасно. Зокрема, описуються метод підвищення безпеки ZRTP за рахунок автоматичної перевірки аутентифікаційного рядка і метод виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана.

3.1 Метод підвищення безпеки ZRTP за рахунок автоматичної перевірки аутентифікаційного рядка

Протокол Діффі-Хелмана може бути повністю скомпрометований активним зловмисником. Тому при роботі протоколу необхідно забезпечити справжність вихідних даних [36]. З цієї причини протокол обміну ключами Діффі-Хелмана зазвичай застосовують по захищеному каналу передачі даних [37], в якому неможливо виконати підміну переданих повідомлень, або при використанні сертифікатів [38] або довіреної центру сертифікації, якому довіряють обидва кореспондента для цілей аутентифікації.

У разі необхідності встановити захищене з'єднання між двома кореспондентами, вони, по-перше, можуть не мати спільних сертифікатів (тобто сертифікатів, що мають один і той же кореневий довірений центр), не мати загального довіреного центру сертифікації або розподілу ключів, а також можуть не мати захищеного каналу зв'язку між собою.

При наявності у кореспондентів сертифікатів, підписаних різними центрами сертифікації, неможливо перевірити справжність сертифікату, так як кожен з кореспондентів може не довіряти центру сертифікації респондента.

Для організації захищеного з'єднання між кореспондентами також потрібно виконати розподіл ключового матеріалу для цього з'єднання.

Кореспонденти можуть використовувати симетричне або асиметричне шифрування. При використанні симетричного шифрування - один з кореспондентів повинен передати іншому секретний ключ. Якщо цей ключ стане відомим порушнику - передані в процесі сеансу зв'язку повідомлення будуть розшифровані порушником. При використанні асиметричного шифрування - інформація не буде прочитана порушником навіть в разі перехоплення повідомлень. Однак - при обміні ключами для організації захищеного з'єднання у кореспондентів не буде можливості упевнитися - що відкритий ключ передається між ними без модифікації порушником, як представлено на рис. 3.1.

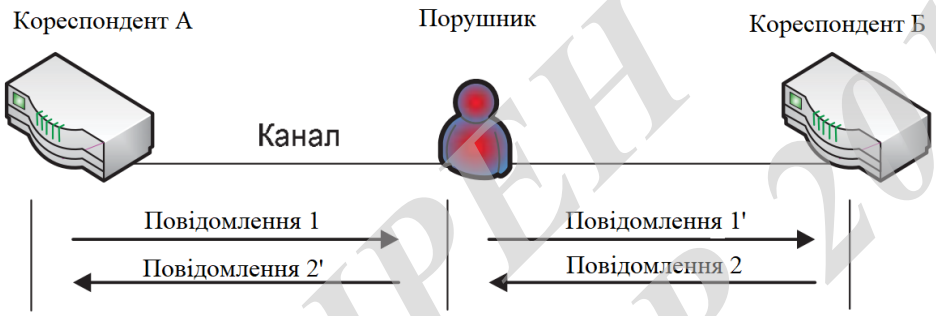


Рисунок 3.1 – MITM при використанні асиметричного шифрування

Також варто відзначити, що відкритий і закритий ключі мають велику довжину і їх передача між кореспондентами в словесному або письмовому вигляді ускладнена.

Для підвищення безпеки пропонується використовувати два методи:

- підвищення безпеки за рахунок автоматизації перевірки аутентифікаційного рядка по другому каналу зв'язку;
- використання двох і більше каналів зв'язку для виконання протоколу розподілу ключів.

Захист від порушника в режимі клієнт-клієнт виконується за рахунок перевірки аутентифікаційного рядка, який передається по голосовому каналу в ручному режимі. Голосовий канал в цьому випадку є додатковим каналом зв'язку по відношенню до IP-каналу. Доцільно автоматизувати процес перевірки SAS. Існуючий метод не безпечний, тому що використовується один канал зв'язку, а сучасні засоби аналізу і синтезу мови дозволяють виконувати автоматичне вирізання рядка і заміну на рядок, синтезовану порушником.

Проведене практичне дослідження показало, що існує висока ймовірність наявності між кореспондентами незалежних непересічних маршрутів при використанні декількох каналів зв'язку. В основі пропонованих

протоколів використано перевага легітимних кореспондентів над нелегітимними, що полягає в тому, що тільки легальні кореспонденти можуть отримувати повідомлення з двох і більше каналах зв'язку одночасно, володіючи знаннями про IP-адреси кореспондентів, при цьому ця інформація не є секретною для порушника. Слід зазначити, що метод модернізації протоколів розподілу ключів розглядається, як підвищення безпеки, але при цьому не забезпечує 100% достовірність.

Розглядаються кілька можливих варіантів модернізації протоколу розподілу ключів при використанні двох або трьох каналів зв'язку. В якості критеріїв оцінки використовуються величини наступних ймовірностей:

- Імовірність успішної атаки MITM $P_{УА}$;
- Імовірність виявлення атаки MITM $P_{ОН}$;
- Імовірність успішного генерування спільної таємниці $P_{УК}$.

Протокол ZRTP має механізм захисту від MITM, виражений у вербальній перевірці короткою аутентифікаційного рядка SAS по мовному каналу між обома кореспондентами. Це означає, що після виконання протоколу ZRTP і встановлення мовного каналу в топології клієнт-клієнт без сервера кореспонденти отримують значення SAS - обчислену текстовий рядок з комбінації символів.

SAS= f(hash(Hello респондента||Commit||DHPart1||DHPart2).

Один з кореспондентів вимовляє аутентифікаційний рядок по сталому мовному канал. Другий кореспондент звіряє SAS на своєму терміналі зі значенням, отриманим по мовному каналу. Якщо SAS збігаються, значить, не має місце атака MITM, або має місце атака з підробкою SAS по мовному каналу зв'язку. Якщо SAS розрізняються - значить, має місце атака MITM в каналі передачі даних. Таким чином, при з'єднанні двох кореспондентів без участі сервера - аутентифікація виконується за рахунок знання кореспондентом голосу другого кореспондента, а також за рахунок неспотвореної передачі інформації по двох каналах - по мовному каналу SRTP і каналу передачі даних.

Сучасні технології досить просто дозволяють виконувати як аналіз голосу кореспондентів, так і синтез мови, в тому числі, синтез мови для цілей підробки голосу. Розглядаються два варіанти:

1. Кореспонденти знають голос один одного.

2. Кореспонденти не знають голос один одного.

У першому випадку, при з'єднанні викликає кореспондент, як правило, вимовляє привітання і ім'я викликається сторони. Після цього виконується вербальна перевірка SAS. Зібраних голосових даних може бути досить для синтезу мови кореспондента для заміни одних слів на інші з метою підміни

SAS в голосовому каналі. В цьому випадку - перевірка SAS пройде успішно навіть при наявності атаки MITM (рис. 3.2).

У другому випадку, коли кореспонденти не знають голосу один одного, не потрібно збору даних, так як синтез можна виконувати з використанням будь-якого голосу.

В якості модернізації протоколу ZRTP пропонується додавання автоматизованої перевірки аутентифікаційного рядка SAS. При використанні двох і більше каналів зв'язку, перевірка дозволить виявити порушника.

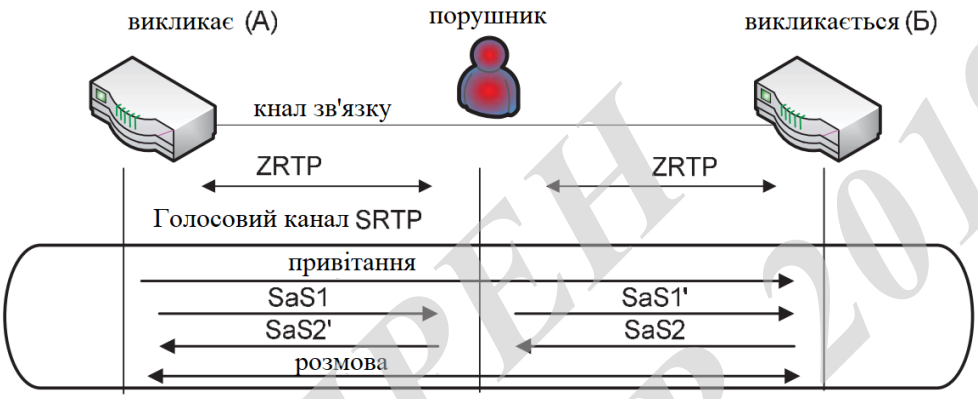


Рисунок 3.2 – Порушник, який виконує заміну SAS в голосовому каналі зв'язку

Інформація про IP-адреси може бути передана між кореспондентами по телефону, по електронній пошті, при особистій зустрічі, листом і іншими доступними способами. Відмінною особливістю є те, що інформація про IP-адреси не є секретною інформацією для порушника і може бути передана по відкритих каналах зв'язку, в той час, як пароль для симетричного шифрування є секретним і розголошення призведе до можливості порушника дешифрувати передану інформацію. У порівнянні з довжиною асиметричного ключа, загальна довжина двох IPv4 або IPv6 адрес набагато менше. При перехопленні асиметричного ключа - порушник може відправляти дані легітимному респонденту так само, як і легітимний кореспондент.

При використанні IP-адрес додатковим заходом для підвищення безпеки є перевірка IP-адрес відправника повідомлень респондентом, а також можливість отримання всіх повідомлень, відправлених по двох каналах зв'язку, тільки легітимними респондентами при відсутності атаки MITM одночасно в декількох каналах.

Даний метод підвищення безпеки ZRTP вимагає передачі всього одного повідомлення від кожного з кореспондентів по додатковому каналу зв’язку. В

якості другого каналу зв'язку може виступати не обов'язково канал передачі даних, але і SMS, MMS транспорт.

Особливістю підходу також є невисока складність розробки програмної реалізації протоколу за рахунок використання існуючих бібліотек [30]. Значення SAS передається в додаток за результатами виконання протоколу ZRTP. Досить додатково передати цей параметр кореспонденту по другому каналу зв'язку у відкритому або зашифрованому вигляді для реалізації автоматичної перевірки.

Недоліком методу підвищення безпеки у вигляді автоматизації перевірки SAS є виявлення порушника в каналі зв'язку безпосередньо після успішного виконання протоколу, а не під час виконання.

Для оцінки можливості застосування декількох каналів зв'язку для цілей підвищення безпеки необхідно вирішити такі завдання:

• оцінити ймовірність наявності загальної точки в двох і більше каналах зв'язку при використанні різних операторів зв'язку між кореспондентами;

• розробити алгоритм прийняття рішення про наявність порушника і оцінка ймовірності помилки можливих рішень.

Оцінка ймовірності виконана в розділі 3.2.2 поточної глави і показує високе значення ймовірності наявності двох і більше незалежних каналів зв'язку між кореспондентами, підключеними до різних операторів зв'язку.

Пропонується використовувати наступний алгоритм автоматичної перевірки SAS. Кореспонденти A і B виконують попередній обмін інформацією про IP-адреси IP_{A1}, IP_{A2}, IP_{B1}, IP_{B2}, де IP_{A1}, IP_{A2} – адреси кореспондента A, IP_{B1}, IP_{B2} – адреси кореспондента B, а також налаштовують таблицю маршрутизації. Для установки захищеного з'єднання, кореспонденти A і B, виконують протокол ZRTP через канал зв'язку IP_{A1} - IP_{B1} , в результаті чого кожен обчислює значення SAS (рис. 3.3). Кореспондент A відправляє SAS_A по каналу зв'язку IP_{A2} - IP_{B2} кореспонденту B.

Кореспондент B отримує SAS_A'. Кореспондент B посилає SAS_B через канал зв'язку IP_{A2} - IP_{B2} кореспонденту A. Кореспондент A отримує SAS_B'.

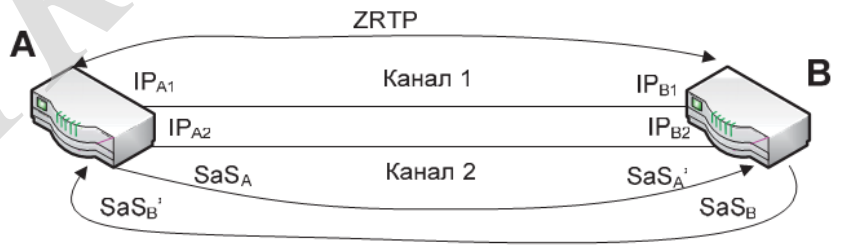


Рисунок 3.3 – Механізм автоматичної перевірки SAS

Кореспондент В виконує порівняння SAS_A’ и SAS_B. Якщо вони збігаються - значить відсутній активний порушник в двох каналах зв'язку, або присутній один і той же активний порушник одночасно в двох каналах зв'язку. Якщо значення SAS не збігаються, кореспондент В отримує повідомлення від терміналу про наявність порушника в каналі зв'язку.

Кореспондент А виконує порівняння SAS_A и SAS_B’. Якщо вони збігаються

- значить відсутній активний порушник в двох каналах зв'язку, або присутній один і той же активний порушник одночасно в двох каналах зв'язку. Якщо значення SAS не збігаються, кореспондент А отримує повідомлення від терміналу про наявність порушника в каналі зв'язку.

Фактично - протокол дозволяє виявити наявність активного порушника, який працює в одному з двох каналів зв'язку.

Виконується розрахунок ймовірностей подій: $P_{УА}$, $P_{ОН}$, $P_{УК}$.

Під успішної атакою розуміється подія, що порушник успішно реалізував атаку MITM, виконавши обмін ключами з обома кореспондентами при використанні декількох каналів зв'язку, не знайшовши себе при проведенні атаки. Це можливо лише в одному випадку, якщо один і той же порушник може контролювати всі використовувані кореспондентами канали зв'язку і виконувати синхронну модифікацію переданих повідомлень в кожному з каналів зв'язку. Імовірність успішної атаки $P_{УА\_SAS}$ для протоколу с автоматичною перевіркою SAS відповідає ймовірності події, що порушник може прослуховувати і виконувати модифікацію повідомлень в двох каналах зв'язку одночасно.

$$P_{УА2\_SAS} = (P_{Н1К})^2 . \quad (3.1)$$

Під подією виявлення порушника визначається подія, що порушник виявлений кореспондентами в одному з використовуваних каналів зв'язку. Виявлення порушника дозволяє користувачам визначити, що може бути вироблений компрометувати ключ, який дозволить порушнику дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію переданих повідомлень

Ймовірність виявлення порушника $P_{ОН\_SAS}$ для протоколу с автоматичною перевіркою SAS відповідає ймовірності знаходження порушника в одному каналі зв'язку при відсутності порушника в іншому каналі зв'язку.

Нехай сеанс ZRTP виконується по першому каналу зв'язку.

Імовірність наявності порушника в першому каналі зв'язку при відсутності порушника в другому каналі зв'язку матиме вигляд:

$$P_{ПОР1К\_НІ\_ПОР2К}=(1- P_{НІК})\, P_{НІК}. \quad (3.2)$$

Імовірність наявності порушника в другому каналі зв'язку при відсутності порушника в першому каналі зв'язку буде визначатися по аналогічно до формули 3.2:

$$P_{ОН\_SAS}= 2(1- P_{НІК})\, P_{НІК}. \quad (3.3)$$

Під подією успішної вироблення ключа розуміється, що порушника не виявлено ні в одному з каналів зв'язку і кореспонденти виробляють ключ для подальшої роботи і шифрування переданих даних. Подія можливо тільки в разі, якщо порушника немає ні в одному каналі зв'язку.

Імовірність успішної вироблення ключа $P_{УК\_SAS}$ для протоколу з автоматичною перевіркою SAS відповідає вірогідності відсутності порушника в обох каналах зв'язку. Імовірність відсутності порушника в одному каналі зв'язку $P_{НІ\_ПОР}$ має вид:

$$P_{НІ\_ПОР}=1- P_{НІК}. \quad (3.4)$$

Тоді:

$$P_{УК\_SAS} = P_{НІ\_ПОР}^{\ 2} = (1- P_{НІК})^2. \quad (3.5)$$

Однак, протокол з автоматичною перевіркою SAS не дозволяє визначити, який саме з каналів зв'язку атакує порушник. Також наявність порушника визначається тільки при повному виконанні протоколу і не може бути детерміновано протягом виконання протоколу. З цієї причини - слід розглянути додаткові варіанти модернізації протоколу ZRTP, в тому числі варіанти, позбавлені вище описаних недоліків.

3.2 Метод виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі- Хелмана

3.2.1 Оцінки ймовірностей результатів розподілу ключів при використанні декількох каналів зв'язку

Для підвищення безпеки пропонується застосовувати метод виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-

Хелмана, що дозволяє виконувати розподіл ключів з використанням декількох каналів зв'язку одночасно (рис. 3.6) і виявляти активного порушника.

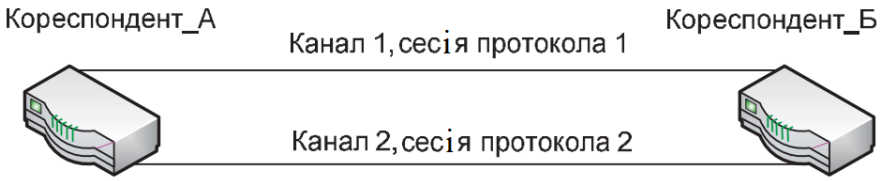


Рисунок 3.6 – Використання кілька каналів зв'язку для розподілу ключів

В даний час наявність двох і більше підключень у одного кореспондента досить поширене. Окремим випадком може послужити користувач, який має бездротове підключення через 3G/4G модем і одночасно має підключення до мережі інтернет від оператора дротового широкосмугової мережі передачі даних.

Нехай існують два кореспондента, що мають кожен по два і більше підключень до глобальної мережі Інтернет. Кожне підключення виконується через різних операторів зв'язку. Обидва кореспондента мають публічний IP-адресу в кожному використовуваному каналі зв'язку. Кожен з кореспондентів передає іншому свої IP-адреси, які будуть використовуватися для встановлення зв'язку між кореспондентами. Дані можуть бути передані в словесній бесіді, при зустрічі, за допомогою електронної пошти або поштового відправлення тощо, а також з використанням комбінації вищеописаних засобів зв'язку.

Реалізація роботи протоколу ZRTP за двома і більше каналам зв'язку вимагає інтеграцію багатоканального протоколу з протоколами SIP / RTP для вирішення наступних технічних завдань:

- визначення додаткових IP-адрес, а також UDP портів для виконання другої сесії протоколу, а також передачу цих параметрів в сам протокол, клас протоколу або функцію протоколу;
- реалізація перевірки отриманих повідомлень Діффі-Хелмана по різних каналах зв'язку і виконання подальших дій за результатами перевірки;
- інтеграцію з SIP і RTP протоколом, так як оригінальний ZRTP протокол використовує узгоджені IP і UDP порти з цих протоколів.

У той же час - реалізація одночасного обміну повідомленнями ZRTP по двох каналах зв'язку, а також реалізація логіки перевірки співпадаючих повідомлень може зажадати набагато більших ресурсів.

Для реалізації двоканального методу (2К) підвищення безпеки по двох каналах зв'язку будуть передаватися однакові повідомлення обміну Діффі-Хелмана. Ініціатор (викликає кореспондент, який бажає встановити захищене з'єднання) відправляє по двох каналах зв'язку два однакових повідомлення. Респондент отримує повідомлення, проводить необхідні обчислення, а також перевіряє, що отримані однакові повідомлення. У разі, якщо отримані різні повідомлення - має місце наявність активного порушника в одному з каналів, що виконує атаку MITM. Респондент відповідає, відправляючи по двох каналах зв'язку у відповідь повідомлення Діффі-Хелмана. Ініціатор отримує повідомлення і перевіряє - чи є повідомлення однаковими. Якщо повідомлення однакові - значить, або відсутній активний порушник в обох каналах зв'язку, або існує один і той же активний порушник в обох каналах зв'язку. Взаємодія кореспондентів при використанні модифікації ZRTP представлена на рис. 3.7.

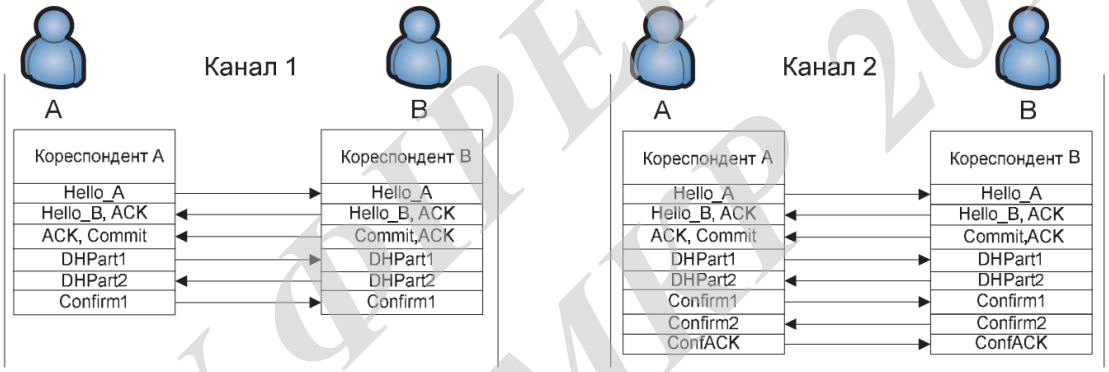


Рисунок 3.7 – Варіант взаємодії кореспондентів при використанні модернізованого протоколу ZRTP в режимі двоканального обміну

Вводиться ймовірність РН1К, що порушник може виконувати атаку MITM в одному з каналів зв'язку [33]. Ця ж ймовірність буде відповідати невдалій спробі виконання атаки MITM, так як виявляється наведеним вище протоколом [34].

Виконується розрахунок ймовірностей подій: $P_{УА}$, $P_{ОН}$, $P_{УК}$.

Під успішної атакою розуміється подія, що порушник реалізував атаку MITM, виконавши обмін ключами з обома кореспондентами по декількох каналах зв'язку. При цьому, порушник не виявив себе під час проведення атаки. Це стає можливим лише в разі, коли один і той же порушник може контролювати всі використовувані кореспондентами канали зв'язку і виконувати синхронну модифікацію переданих повідомлень в кожному з каналів зв'язку.

Імовірність успішної атаки $P_{УА2}$ для двоканального протоколу відповідає $P_{Н2К}$ - ймовірності події, що порушник може прослуховувати і виконувати модифікацію повідомлень в 2 каналах зв'язку одночасно.

$$P_{УА2}= P_{Н2К} = (P_{Н1К})^2. \quad (3.6)$$

Виявлення порушника дозволяє користувачам визначити, що може бути вироблений компрометувати ключ, що дозволяє дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію повідомлень. Ймовірність виявлення порушника залежить від числа використовуваних каналів зв'язку, а також від здатності алгоритму розподілу ключів визначити існування порушника в конкретному або конкретних каналах зв'язку з сукупності використовуваних.

Ймовірність виявлення порушника $P_{ОН2}$ для двоканального методу відповідає ймовірності знаходження порушника в одному каналі зв'язку при відсутності порушника в іншому каналі зв'язку.

Імовірність наявності порушника в першому каналі зв'язку при відсутності порушника в другому каналі зв'язку матиме вигляд:

$$P_{ПОР1К\_НІ\_ПОР2К}=(1- P_{Н1К}) P_{Н1К} . \quad (3.7)$$

Імовірність наявності порушника в другому каналі зв'язку при відсутності порушника в першому каналі зв'язку матиме вигляд:

$$P_{НІ\_ПОР1К\_ПОР2К}=(1- P_{Н1К}) P_{Н1К}= P_{Н1К}- (P_{Н1К})^2; \quad (3.8)$$

$$P_{ОН2} = P_{ПОР1К\_НІ\_ПОР2К} + P_{НІ\_ПОР1К\_ПОР2К} =2(1- P_{Н1К}) P_{Н1К}. \quad (3.9)$$

Під успішним виробленням ключа розуміється подія, що порушника не виявлено ні в одному каналі зв'язку і кореспондентами вироблений ключ для шифрування даних, що передаються. Це можливо тільки в разі відсутності порушника в застосовуваних каналах зв'язку, або при використанні здатності алгоритму розподілу ключів визначати точне знаходження порушника в конкретному або конкретних каналах зв'язку з сукупності використовуваних.

Імовірність успішної вироблення ключа $P_{УК2}$ для двоканального протоколу відповідає вірогідності відсутності порушника в обох каналах зв'язку. Імовірність відсутності порушника в одному каналі зв'язку $P_{НІ\_ПОР}$:

$$P_{НІ\_ПОР} =1- P_{Н1К} ; \quad (3.10)$$

Тоді:

$$P_{УК2} = P_{НІ\_ПОР2} = (1- P_{Н1К})^2 . \quad (3.11)$$

Розглядається інший варіант методу виявлення порушника з використанням трьох каналів передачі даних.

Нехай по трьох каналах зв'язку передаються однакові повідомлення обміну Діффі-Хелмана. Приклад взаємодії кореспондентів при використанні модернізованого протоколу ZRTP наведено на рис. 3.8.

Ініціатор відправляє по трьох каналах зв'язку три однакових повідомлення. Респондент отримує повідомлення, проводить необхідні обчислення, а також перевіряє, що отримані однакові повідомлення по всіх трьох каналах зв'язку. У разі, якщо отримані різні повідомлення, має місце наявність активного порушника, що виконує атаку MITM, або порушник контролює одночасно на три канали зв'язку.

Респондент відповідає, відправляючи по трьох каналах зв'язку у відповідь повідомлення Діффі-Хелмана. Ініціатор отримує повідомлення і перевіряє - чи є повідомлення однаковими.

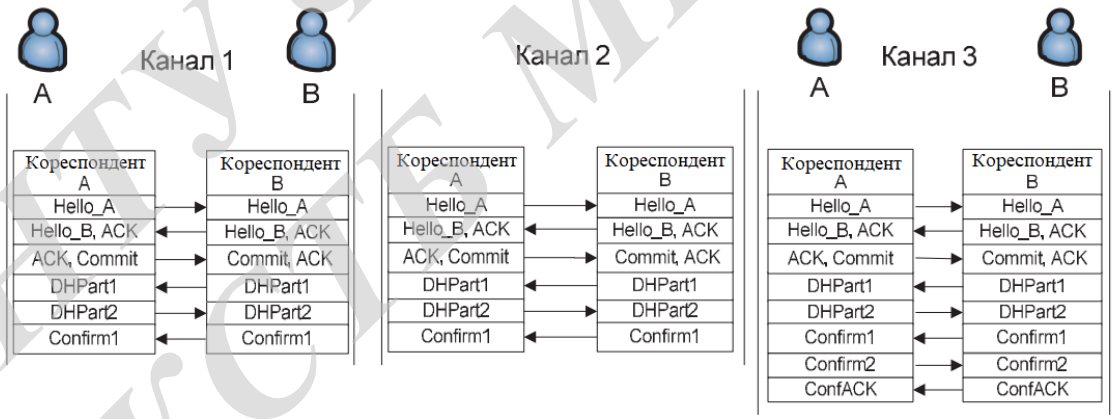


Рисунок 3.8 – Варіант взаємодії кореспондентів при використанні модернізованого протоколу ZRTP при роботі одночасно по трьох каналах зв'язку.

Можливі кілька варіантів роботи протоколу при використанні методу виявлення порушника:

• Якщо повідомлення однакові - значить, або відсутній активний порушник у всіх каналах зв'язку, або існує активний порушник у всіх трьох каналах зв'язку.

• Якщо одне повідомлення відрізняється від інших, значить або присутній один активний порушник в цьому каналі зв'язку, або присутні два порушника в двох інших каналах зв'язку.

• Якщо всі повідомлення різні, значить, присутні два окремо працюючих порушника, що не мають між собою каналу зв'язку.

Таким чином, протокол дозволяє:

• при наявності одного порушника в одному з трьох каналів зв'язку визначити канал з порушником;

• при наявності порушника в двох каналах зв'язку виявити наявність порушника, без визначення каналів зв'язку, що містять порушника.

Однак, протокол не дозволяє при знаходженні порушника в трьох каналах зв'язку визначити наявність порушника. Відповідно, можна виділити два режими роботи методу підвищення безпеки:

• ОН: режим роботи з виявленням порушника (3-ОН);

• ІН: режим роботи з виключенням порушника (3-ІН).

При роботі в режимі ОН в разі виявлення відмінності хоча б одного з трьох повідомлень - протокол завершується з помилкою, повідомляючи користувача про наявність порушника в каналі зв'язку.

У разі роботи в режимі ІН при виявленні відмінності одного з трьох повідомлень - формується повідомляти про наявність порушника в конкретному каналі зв'язку, при цьому протокол продовжує роботу і врахову повідомлення лише з тих каналів зв'язку, де не виявлено порушник. Так забезпечується правильне виключення порушника. Імовірність правильного виключення порушника $P_{ПрІ}$ для трьохканального протоколу відповідає події знаходження порушника в одному з каналів зв'язку при його відсутності в двох інших каналах.

$$P_{ПрІ} = 3\, P_{Н1К}\, (1- P_{Н1К})^2. \qquad (3.12)$$

Однак, при наявності активного порушника одночасно в двох каналах зв'язку з трьох можливих, а також синхронної модифікації повідомлень в двох каналах зв'язку порушником, механізм виключення може викликати некоректне визначення каналу з порушником, що призведе до помилкового вибору двох каналів, що містять порушника, як надійних . Це дозволить порушнику успішно виконати обмін ключами з кореспондентами, здійснивши успішну атаку MITM.

Імовірність помилкового виключення відповідає ймовірності події, що порушник перебуває одночасно в двох каналах зв'язку.

$$P_{ПомІ} = 3\, P_{Н1К}^2\, (1- P_{Н1К})\ . \qquad (3.13)$$

Ця ймовірність буде також бути складовою частиною ймовірності успішної атаки MITM.

Виконується розрахунок ймовірностей для протоколу трьохканального обміну в режимі ОН $P_{УА,}$ $P_{ОН,}$ $P_{УК}$.

Імовірність успішної атаки $P_{УАЗ\_ОН}$ для трьохканального протоколу в режимі ОН відповідає $P_{НЗК}$ - ймовірності події, що порушник може прослуховувати і виконувати модифікацію повідомлень в трьох каналах зв'язку одночасно.

$$P_{УАЗ\_ОН} = P_{НЗК} = (P_{Н1К})^3\ . \qquad (3.14)$$

Ймовірність виявлення порушника $P_{ОНЗ\_ОН}$ для трьохканального протоколу в режимі ОН відповідає ймовірності знаходження порушника в одному або двох каналах зв'язку при відсутності порушника в іншому каналі зв'язку. Імовірність наявності порушника в одному з каналів зв'язку при відсутності порушника в двох інших каналах зв'язку буде мати вигляд:

$$P_{\ ПОР1К\_НІ\_ПОР23К} = 3(1- P_{Н1К})^2\, P_{Н1К}\ . \qquad (3.15)$$

Імовірність наявності порушника в двох з трьох каналів зв’язку при відсутності порушника в одному з каналів зв’язку буде мати вигляд:

$$P_{\ НІ\_ПОР1К\_ПОР23К} = 3(1- P_{Н1К})\, P_{Н1К}^2\ ; \qquad (3.16)$$

$$P_{ОНЗ\_ОН} = P_{ПОР1К\_НЕТ\_ПОР23К} + P_{НІ\_ПОР1К\_ПОР23К} = \\ = 3(1- P_{Н1К})^2\, P_{Н1К} + 3(1- P_{Н1К})\, P_{Н1К}^2\ . \qquad (3.17)$$

Імовірність успішної вироблення ключа $P_{УКЗ\_ОН}$ для трьохканального протоколу в режимі ОН відповідає вірогідності відсутності порушника в трьох каналах зв'язку:

$$P_{УКЗ\_ОН} = P_{\ НІ\_ПОРЗ} = (1- P_{Н1К})^3\ . \qquad (3.18)$$

Виконується розрахунок ймовірностей $P_{УА,}$ $P_{ОН,}$ $P_{УК}$ для протоколу трьохканального обміну в режимі ІН. Імовірність успішної атаки $P_{УАЗ\_ІН}$ для

трьохканального протоколу відповідає ймовірності події, що порушник може прослуховувати і виконувати модифікацію повідомлень в двох або трьох каналах зв'язку одночасно.

$$P_{УАЗ\_ІН=}(P_{Н1К})^3 + 3(1- P_{Н1К})\, P_{Н1К}^2 . \quad (3.19)$$

Ймовірність виявлення порушника РОНЗ_ІН для трьохканального протоколу в режимі ІН відповідає ймовірності знаходження порушника в одному каналі зв'язку при відсутності порушника в двох інших каналах зв'язку і буде мати вигляд:

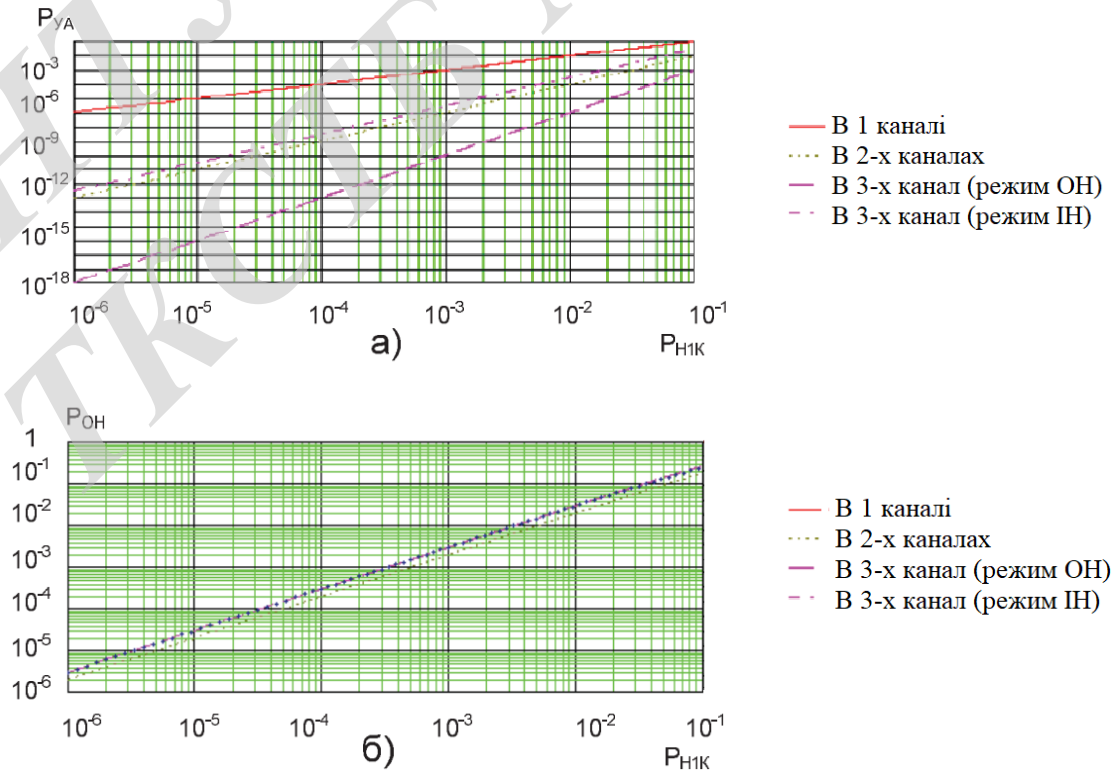
$$P_{ОНЗ\_ІН} = 3(1- P_{Н1К})^2\, P_{Н1К} . \quad (3.20)$$

Імовірність успішної вироблення ключа РУКЗ_ІН для трьохканального протоколу в режимі ІН відповідає вірогідності відсутності порушника в двох або трьох каналах зв'язку:

$$P_{УКЗ\_ІН}=(1- P_{Н1К})^3 + 3(1- P_{Н1К})^2\, P_{Н1К} . \quad (3.21)$$

Для порівняння, для простого протоколу Діффі-Хелмана, що працює по одному каналу, ймовірності матимуть вигляд: $P_{УА1} = P_{Н1К}$; $P_{ОН2}= 0$; $P_{УК} =1 - P_{Н1К}$.

Отримані залежності для ймовірностей представлені на рис. 3.9а-3.9в



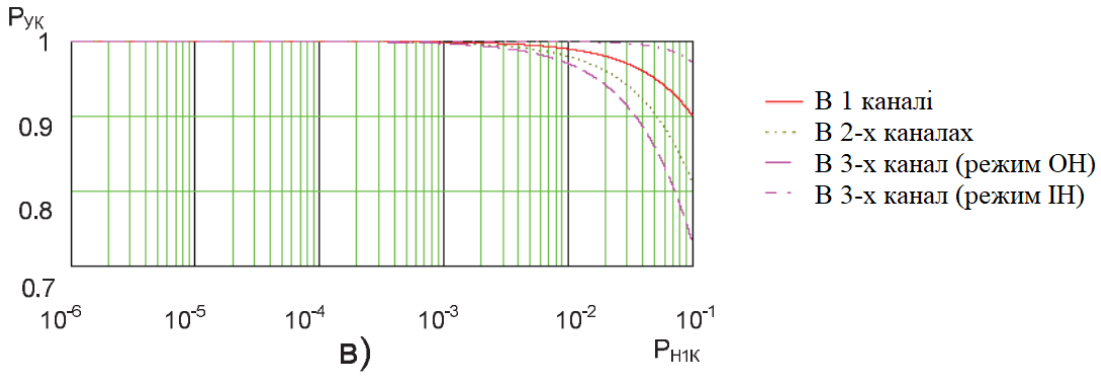


Рисунок 3.9 – Порівняльні характеристики ПРК в чотирьох режимах: а) ймовірність успішної атаки MITM б) імовірність виявлення порушника в) ймовірність успішної вироблення ключа

Модифікація протоколу для роботи по декількох незалежних каналах суттєво зменшує ймовірність успішної атаки MITM. Ефективність захисту зростає зі збільшенням числа незалежних каналів. Модифікація в режимі виявлення порушника з використанням трьох каналів зв'язку має найбільшу ймовірність виявлення порушника, а також найменшу ймовірність успішної атаки порушника. Модифікація в режимі виключення порушника із застосуванням трьох каналів має найбільшу ймовірність успішної вироблення загального секрету між кореспондентами. Для реалізації вибирається одна з модифікацій в залежності від цілей і доступних ресурсів, виражених в числі доступних каналів зв'язку.

Дослідження показують, що при підключенні кореспондентів до кількох операторам зв'язку незалежні двійки і трійки маршрутів є завжди. Імовірність успішного формування загального ключа в багатоканальної схемою з виявленням порушника зменшується незначно. У схемі з виключенням порушника дана ймовірність збільшується, але при використанні трас великої протяжності можливо збіг вузлів проходження маршрутів, що може знизити ефективність роботи модифікованого протоколу.

3.3 Висновки до розділу 3

Запропоновано метод виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана, що полягає у використанні декількох відкритих каналів зв'язку і опублікований в [35]. Метод відрізняється від існуючих зниженою вірогідністю успішної атаки MITM, а також наявністю механізму визначення активного порушника в каналі зв'язку навіть при відсутності заздалегідь розподіленого загального секрету. Однак,

даний метод накладає обмеження на використовувані канали зв'язку, виражене в тому, що канали зв'язку повинні бути незалежні.

Розроблено методику оцінки ймовірності збігу маршрутів в глобальній мережі. Методика дозволяє кількісно оцінити ймовірність існування спільних точок у пар і трійок наявних маршрутів. Показано, що ймовірність наявності двох незалежних каналів зв'язку досить велика, але її значення зменшується при збільшенні відстані між точками підключення.

Запропоновано метод підвищення безпеки ПРК, що відрізняється від існуючого методу вербальної перевірки SAS автоматизацією процесу виявлення порушника, що не вимагає участі користувачів.

4 РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПОЛІПШЕННЯ ЙМОВІРНОСНО-ЧАСОВИХ ХАРАКТЕРИСТИК ПРОТОКОЛУ ZRTP

Детально принцип розрахунку ВВХ протоколу ZRTP був викладений в розділі 4,1 Відповідно до Наказу Міністерства інформаційних технологій і зв'язку Російської Федерації від 27.09.2007 № 113 «Про затвердження Вимог до організаційно-технічного забезпечення стійкого функціонування мережі зв'язку загального користування» час з моменту отримання призначеним для користувача (крайовим) обладнанням абонента інформації про відповідь від призначеного для користувача (кінцевого) обладнання абонента до моменту встановлення з'єднання між призначеним для користувача (крайовим) обладнанням викликаючого і викликаного абонента (час виконання з'єднання) не повинно перевищувати 1 с в мережі зонового телефонного зв'язку і в мережі міжміського і міжнародного телефонного зв'язку, а також не повинно перевищувати 1,5 с в мережі місцевого телефонного зв'язку [47].

Відповідно до теоретичним розрахунком, а також практичним експериментом при односторонній затримки в лінії понад 100 мс середній час виконання протоколу ZRTP становить близько 0,9 с, а при 150 мс становить 1.2 с, що перевищує встановлену норму. У разі наявності помилок в каналі зв'язку час виконання протоколу також зростає за рахунок необхідності повторної відправки повідомлень.

Таким чином, за певних умов час виконання протоколу ZRTP не задовольняє існуючим нормативам. Відповідно - має сенс виконати модернізацію протоколу для поліпшення параметрів ВВХ.

Протокол можна розділити на кілька етапів:

- узгодження початкових параметрів і умов;
- підготовка до обміну повідомленнями;
- обмін і генерація загального ключа по протоколу Діффі-Хелмана;
- перевірка загального ключа.

На етапі підготовки від одного кореспондента до іншого передається параметр hvi, який розташовується в повідомленні Commit і визначається, як: hvi = hash (DHPart2 || Hello респондента)

Експериментальна оцінка і теоретичні розрахунки показали, що в режимі Діффі-Хелмана протоколу ZRTP загальна довжина повідомлень Commit + Hello порівнянна з довжиною повідомлень DHPart1 або DHPart2. Тому в якості модернізації протоколу пропонується об'єднати повідомлення HelloB + Commit. Після отримання повідомлення Hello_A другий кореспондент уже володіє всіма необхідними даними, щоб вибрати криптографічний набір для продовження роботи протоколу.

Недоліком підходу може бути необхідність вже на першій фазі ZRTP виконати обчислення для протоколу Діффі-Хелмана, що вимагає задіяти обчислювальні ресурси на обладнанні обох кореспондентів. Однак, додатково підхід дозволяє виключити з протоколу останнім повідомлення Conf2ACK. Необхідність повідомлення у вихідному протоколі викликана наявністю незавершеною четвертої фази, де на повідомлення ініціатора Confirm2 респондент повинен відповісти повідомленням. При об'єднанні пакетів Hello + Commit повідомлення DHPart2 буде відповідним для DHPart1, повідомлення Confirm2 буде відповідним для повідомлення Confirm1. При такому підході повідомлення Confirm2 буде відповідним, і не потребуватиме додаткового повідомлення Conf2ACK.

Так в оновленій версії протоколу буде шість повідомлень: два повідомлення Hello і Commit, повідомлення DHPart1 і DHPart2, два повідомлення перевірки виробленого ключа.

Модернізований протокол буде мати сценарій обміну повідомленнями, представлений на рис. 4.1.

Необхідно виконати оцінку ВВХ оновленого протоколу. Граф оновленого протоколу представлений на рис. 4.11. Виконано спрощення графа за аналогією з повною версією протоколу. Спрощений граф представлений на рис. 4.2.

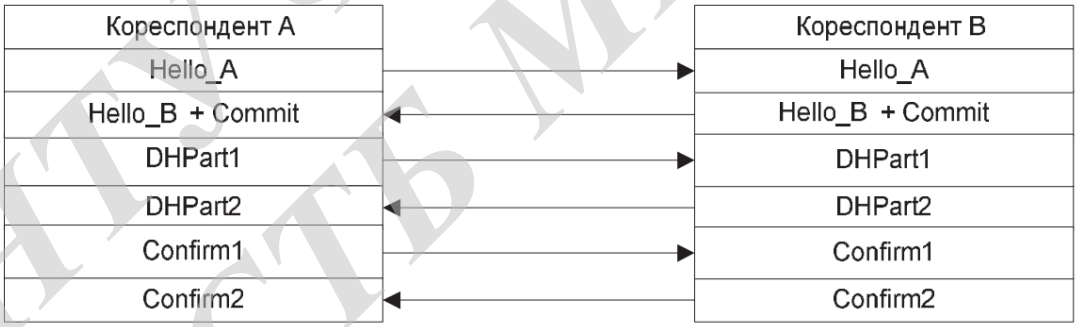


Рисунок 4.1 - Сценарій обміну повідомленнями модернізованого протоколу

Похідна функція гілки успішного завершення протоколу буде визначатися, як:

$$H_{success} = H_{HA0\_20} \bullet H_{HB0\_20} \bullet H_{N0\_10} \bullet H_{N0\_10} \qquad (4.1)$$

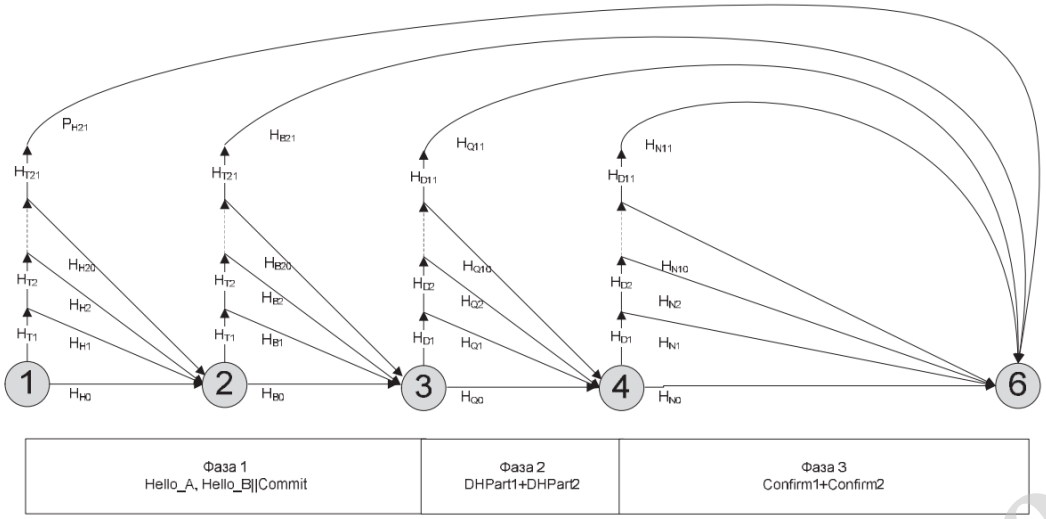


Рисунок 4.2 - Граф оновленого протоколу ZRTP

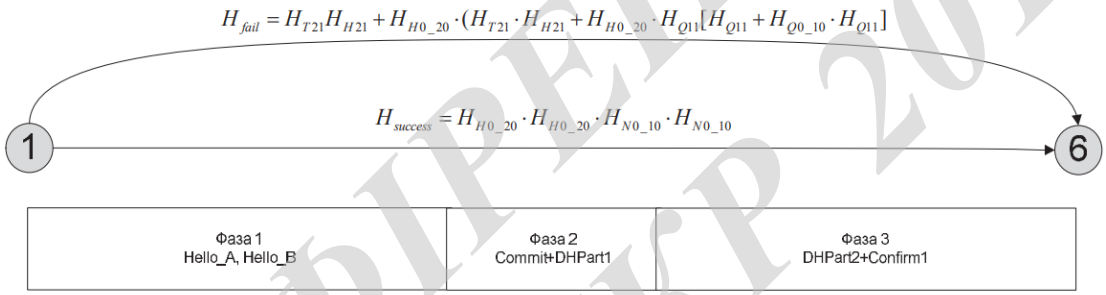


Рисунок 4.3 - Спрощений граф оновленого протоколу ZRTP

Залежність середнього часу успішного виконання оновленого протоколу від p_0 представлена на рис. 4.4. Проводиться оцінка виграшу в модифікованому протоколі в порівнянні з вихідним. Для цього визначається час виконання протоколу при роботі по каналах із затримками при наступних параметрах:

- затримка: 50 мс, 150мс, 300мс;
- p_0: 10-5, 5 * 10-5, 10-4

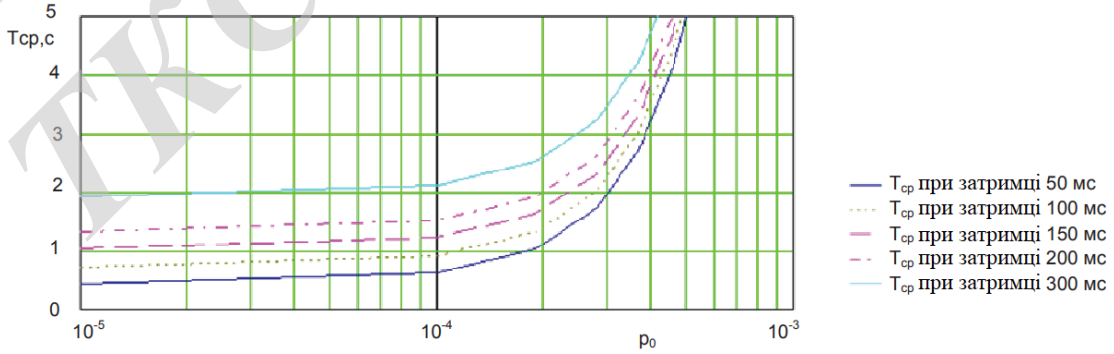


Рисунок 4.4 - Середній час успішного завершення оновленого протоколу ZRTP

Виграш оцінюється, як

$$T_{B1} = T_{ZRTP} - T_{мод1}, \quad (4.2)$$

$$B_{B1} = (T_{ZRTP} - T_{мод1}) / T_{ZRTP}, \quad (4.3)$$

де T_{ZRTP} - середній час виконання вихідного протоколу, с;

$T_{мод1}$- середній час виконання модифікації протоколу, с;

Результати обчислень представлені в табл. 4.1.

Виконується додаткове скорочення числа окремих повідомлень в протоколі ZRTP [54]. Для цього об'єднуються повідомлення Hello_B + Commit + DHPart1, а також повідомлення DHPart2 + Confirm1. Модернізований протокол буде мати сценарій обміну повідомленнями, представлений на рис. 4.5а.

Об'єднання повідомлень призводить до втрати попередньої передачі параметра *hvi*, проте дозволяє зберегти концепцію протоколу і виконати між кореспондентами перевірку отриманого ключа. Спрощення графа наведено на рис. 4.6.

Таблиця 4.1 - Оцінка виграшу середнього часу успішного завершення протоколу ZRTP першої модифікації

d	50мс			150мс			300мс			400мс		
p_0	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}
T_{ZRTP}, с	0,52	0,58	0,7	1,3	1,38	1,5	2,5	2,59	2,7	3,32	3,38	3,51
$T_{мод1}$, с	0,42	0,49	0,62	1,02	1,09	1,2	1,92	1,99	2,09	2,52	2,59	2,72
T_{B1}, с	0,1	0,09	0,08	0,28	0,29	0,3	0,58	0,6	0,61	0,8	0,79	0,79
B_{B1}, %	19,2	15,5	11,4	21,5	21	20	23,2	23,1	22,5	24,1	23,37	22,5

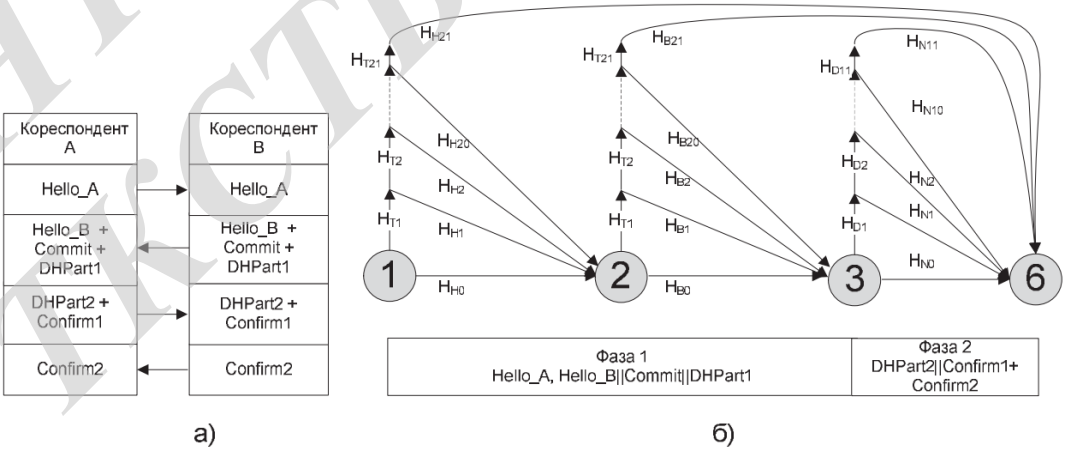


Рисунок 4.5 - Друга модифікація протоколу; а) сценарій обміну повідомленнями б) імовірнісний граф

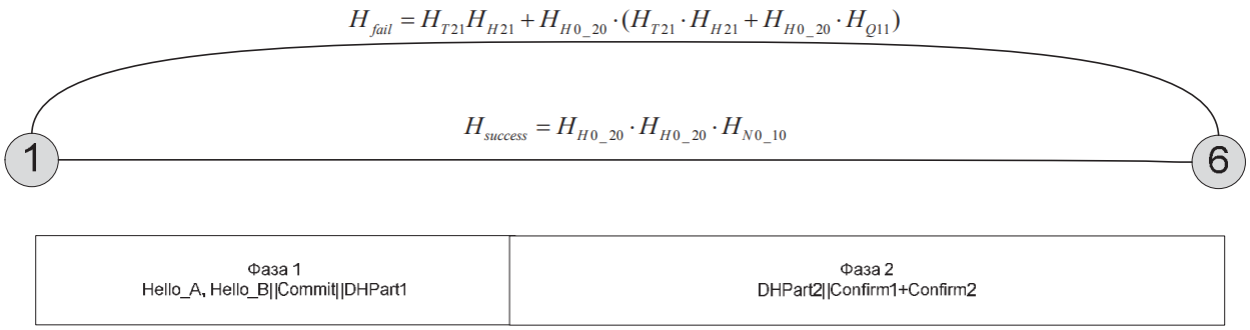


Рисунок 4.6 - Спрощений граф модернізованого протоколу ZRTP

За аналогією обчислено $T_{мод2}$ - середній час виконання другої модифікації протоколу в залежності від затримки і втрати пакетів в каналі зв'язку. Графік наведено на рис. 4.7.

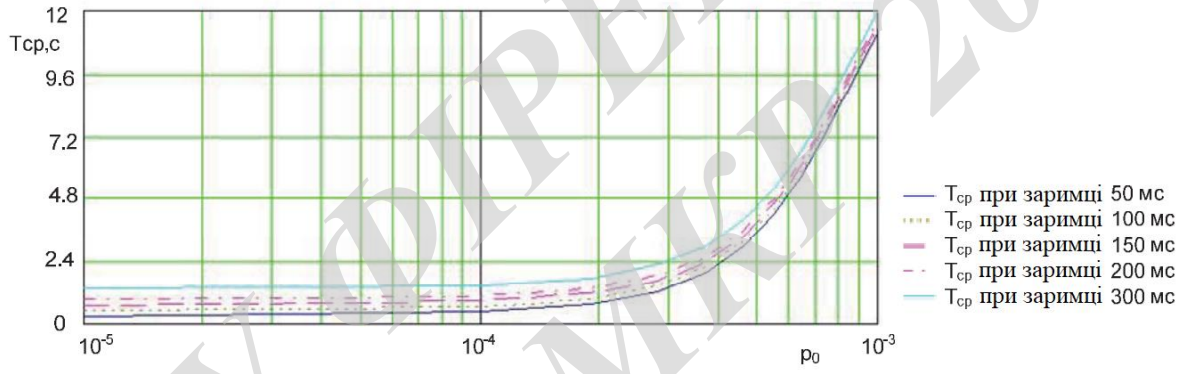


Рисунок 4.7 - Середній час виконання модернізованого протоколу ZRTP другий модифікації

Додатково виконано оцінку виграшу в модифікованому протоколі в порівнянні з вихідним. Для цього визначено час виконання протоколу при роботі по каналах із затримками при наступних параметрах:

- затримка 50 мс, 150мс, 300мс;
- $p_0 = 10^{-5}, 5 * 10^{-5}, 10^{-4}$.

Виграш у часі T_{B2}, що характеризує заощаджений час за рахунок застосування модифікованого протоколу в порівнянні з вихідним, і відносний виграш B_{B2}, що відображає ставлення зекономленого часу до $T_{пром}$, визначені за формулами:

$$T_{B2} = T_{ZRTP} - T_{мод2}, \quad (4.4)$$

$$B_{B2} = (T_{ZRTP} - T_{мод2})/T_{ZRTP}, \quad (4.5)$$

де $T_{мод2}$- середній час виконання другої модифікації протоколу, с;

Результати обчислень представлені в табл. 4.2. Виграш модифікованого протоколу з шести повідомлень перед стандартним протоколом складає від 11% до 24%.

Виграш перед стандартним протоколом модифікованого протоколу, скороченого до чотирьох повідомлень, склав від 35% до 48% відповідно до табл. 4.2. Таким чином, модифікований протокол ZRTP дозволяє працювати по каналах зв'язку з більшою затримкою в порівнянні зі стандартним протоколом ZRTP, при цьому вкладаючись в нормативи для параметрів ТФОП.

Таблиця 4.2 - Оцінка виграшу середнього часу успішного завершення протоколу ZRTP другий модифікації

d	50мс			150мс			300мс			400мс		
p_0	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}
T_{ZRTP}, с	0,52	0,58	0,7	1,3	1,38	1,5	2,5	2,59	2,7	3,32	3,38	3,51
$T_{мод1}$, с	0,31	0,36	0,45	0,71	0,76	0,85	1,31	1,36	1,45	1,71	1,76	1,85
T_{B1}, с	0,20	0,22	0,24	0,58	0,62	0,64	1,18	1,23	1,24	1,60	1,62	1,65
B_{B1}, %	39,4	37,9	35,5	45,0	44,9	43,2	47,4	47,4	46,2	48,3	47,93	47,2

Для підвищення безпеки модифікованого протоколу пропонується використовувати розроблений в третьому розділі метод виявлення порушника. В цьому випадку модифікований протокол виконується по декількох каналах зв'язку одночасно, а час успішного завершення протоколу буде визначатися КС, які мають найбільше значення d. Для виявлення порушника використовується або двоканальний, або трьохканальний режим з виявленням або винятком порушника.

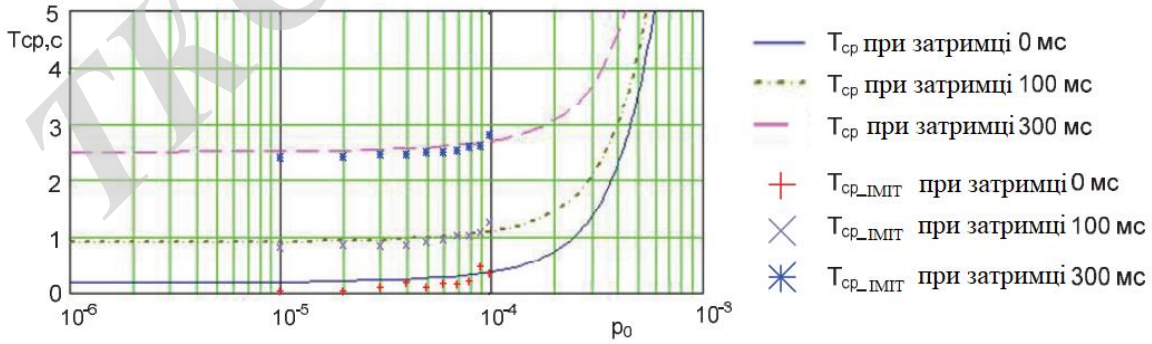


Рисунок 4.8 - Результати імітаційного моделювання $T_{ср}$ для вихідного протоколу ZRTP

Наскільки видно з табл. 4.2, при $p_0 \le 10^{-4}$ і $d \le 300$ мс $T_{мод2} \le 1{,}45$ с. Таким чином, завдання про виконання норм [47] при роботі по каналах зв'язку $d \le 300$ мс вирішена.

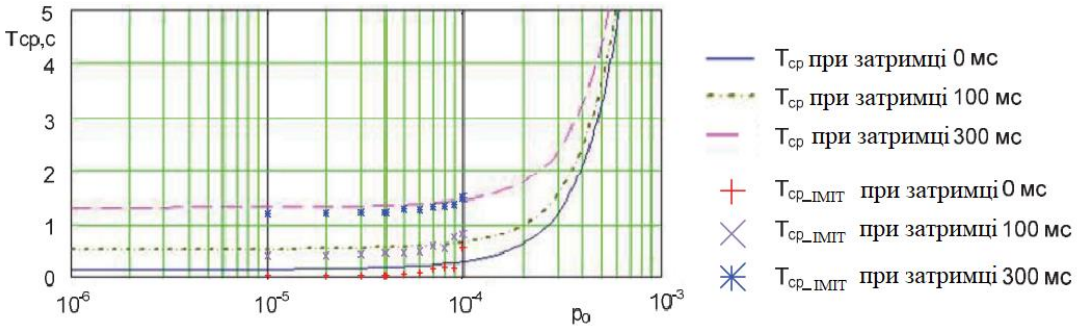


Рисунок 4.9 - Результати імітаційного моделювання $T_{ср}$ для другої модифікації протоколу ZRTP

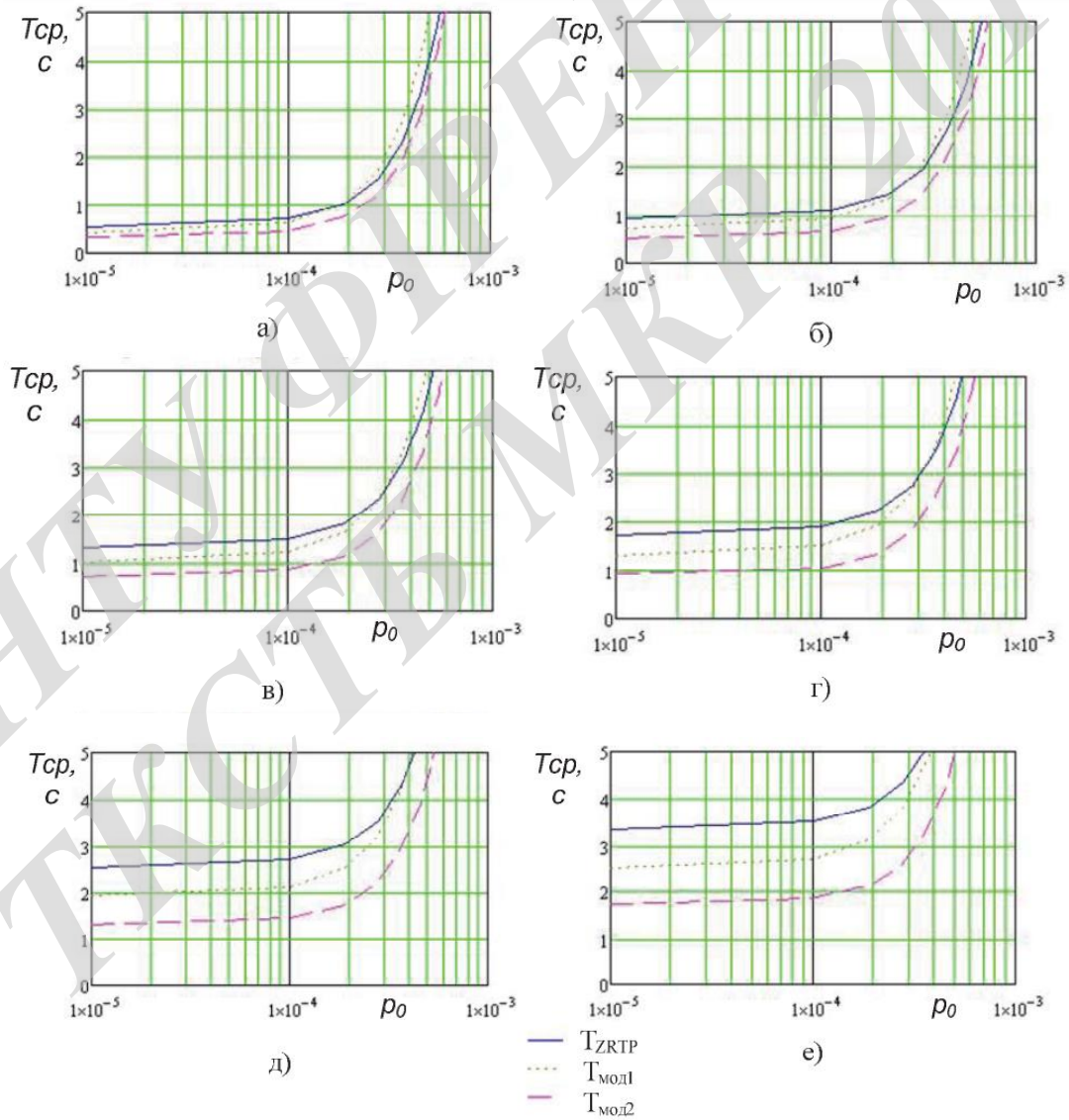


Рисунок 4.10 - Порівняння середнього часу успішного завершення оригінального ZRTP, першої та другої модифікацій ZRTP а) d = 50 мс; б) d = 100 мс; в) d = 150 мс; г) d = 200 мс; д) d = 300 мс; е) d = 400 мс

Виконано імітаційне моделювання для протоколу ZRTP і другий модифікації протоколу, для чого було розроблено додаток на мові програмування PHP. Вихідний код програми наведено в додатку. Результати імітаційного моделювання для вихідного протоколу ZRTP представлені на рис. 4.8.

Результати імітаційного моделювання для другої модифікації протоколу ZRTP представлені на рис. 4.9. Отримані результати підтверджують теоретично отриману залежність.

Порівняння залежностей $T_{мод2}$, $T_{мод2}$, T_{ZRTP} наведено на рис. 4.10.

Виконано імітаційне моделювання для протоколу ZRTP і другий модифікації протоколу, для чого було розроблено додаток на мові програмування PHP. Вихідний код програми наведено в додатку. Результати імітаційного моделювання для вихідного протоколу ZRTP представлені на рис. 4.8.

Результати імітаційного моделювання для другої модифікації протоколу ZRTP представлені на рис. 4.9. Отримані результати підтверджують теоретично отриману залежність.

Порівняння залежностей $T_{мод2}$, $T_{мод2}$, T_{ZRTP} наведено на рис. 4.10.

4.1 Висновки до розділу 4

Представлена методика оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії, що дозволяє визначити ефективність роботи протоколів по каналах з затримками і помилками, оцінюючи середній час, а також ймовірність успішного завершення протоколу. Методика враховує особливості ПРК, пов'язані з обмеженим числом повторів, а також з варіацією затримай в кожному з повторів, і опублікована в [55].

Проведено дослідження ВВХ протоколів DTLS і ZRTP, відповідно до запропонованої методики обчислені середній час успішного завершення і ймовірність успішного завершення.

Для протоколу ZRTP виконана експериментальна оцінка середнього часу успішного завершення, а також виконано порівняння отриманої оцінки з розрахованим за методикою значенням. На підставі порівняння зроблено висновок про збіг теоретичних і практичних результатів.

Показано, що в каналах з високою затримкою протоколу ZRTP потрібно досить великий час на встановлення захищеного з'єднання, що негативно позначається на дотриманні норм на час встановлення голосового каналу між кореспондентами.

Виходячи з вищенаведеного, модернізація протоколу розподілу ключів є актуальним завданням, що дозволяє зберегти переваги протоколу ZRTP, при цьому прискоривши виконання протоколу при роботі по каналах з великими затримками.

Розроблено метод поліпшення тимчасових характеристик криптографічного протоколу ZRTP, що складається у виключенні механізму розподілу ролей ініціатора і респондента, а також в об'єднанні інформаційного блоку даних про підтримувані кореспондентами криптографічних наборах з блоком даних протоколу Діффі-Хелмана.

Виграш В2 в порівнянні з вихідним ZRTP склав від 39,42% до 48,3%, дозволивши при затримці до 300 мс скоротити час успішного виконання протоколу до 1,45, що менше встановленої норми 1.5 с, що дозволяє виконувати цю норму. Поставлена задача вважається розв'язаною. Застосування модифікованого протоколу спільно з запропонованим методом виявлення порушника в режимі ОН дозволяє знизити ймовірність успішної атаки MITM на 3 порядки, тим самим підвищуючи інформаційну безпеку.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Розрахунок витрат на проведення НДДКР з дослідження підвищення інформаційної безпеки IP-телефонії

В техніко-економічному обґрунтуванні представленому в першому розділі даної магістерської кваліфікаційної роботи було приблизно обґрунтовано доцільність проведення НДДКР. Тому в даному розділі будуть проведені більш детальні розрахунки витрат на проведення НДДКР з дослідження та підвищення інформаційної безпеки IP-телефонії.

Для економічного розрахунку проведення НДДКР потрібно скласти кошторис витрат, який передбачає розрахунок визначених основних статей витрат.

Основна заробітна плата дослідників та розробників, яка розраховується за формулою [58]:

$$З_о = \frac{M}{T_р} \cdot t \quad , \tag{5.1}$$

де M – місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ – число робочих днів в місяці, 22 дн;

t – число днів роботи розробника (дослідника).

Проведені розрахунки зводимо до табл. 5.1.

Таблиця 5.1 – Основна заробітна плата дослідників та розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
1. Керівник проекту	11340,00	515,45	22	11340,00
2. Ст. науковий співробітник	10100,00	459,09	15	6886,36
3. Інженер-програміст в сфері захисту інформації	9570,00	435,00	15	6525,00
4. Фахівець-консультант IP-телефонії	10100,00	459,09	5	2295,45
Разом				27046,82

Витрати на основну заробітну плату робітників ($З_р$), що здійснюють підготовку робочих місць та пристроїв необхідних для досліджень, підготовку та формування інформаційних пакетів тощо, розраховуються на основі норм часу, які необхідні для виконання даної роботи, за формулою [58]:

$$З_р = \sum_{1}^{n} t_i \cdot С_i \cdot К_с \quad , \qquad (5.2)$$

де t_i - норма часу (трудомісткість) на виконання конкретної роботи, годин;

n - число робіт по видах та розрядах;

$К_с$ - коефіцієнт співвідношень, який установлений в даний час Генеральною тарифною угодою між Урядом України і профспілками, $К_с$ = 1,13;

$С_i$ - погодинна тарифна ставка робітника відповідного розряду, який виконує відповідну роботу, грн./год.

$С_i$ визначається за формулою [58]:

$$С_i = \frac{М_м \cdot К_i}{Т_р \cdot Т_{зм}} \quad , \qquad (5.3)$$

де, $М_н$ - мінімальна місячна оплата праці, грн., $М_н$ = 4173,00 грн.;

$К_i$ - тарифний коефіцієнт робітника відповідного розряду;

$Т_р$ - число робочих днів в місяці, $Т_р$ = 22 дн;

$Т_{зм}$ - тривалість зміни, $Т_{зм}$ = 8 годин.

Проведені розрахунки внесемо до табл. 5.2.

Таблиця 5.2 – Витрати на основну заробітну плату працівників

Найменування робіт	Трудомісткість, нормо-годин	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн.	Величина оплати, грн.
1. Встановлення допоміжного обладнання	13,50	2	1,1	23,27	442,92
2. Інсталяція програмного забезпечення	16,00	4	1,35	28,56	644,25
3. Встановлення IP модулів	16,00	5	1,7	35,96	811,28
Разом					1898,44

Додаткова заробітна плата розробників, дослідників та працівників, які приймали участь в дослідженнях та розробці НДДКР з дослідження та підвищення інформаційної безпеки IP-телефонії розраховується як 12% від основної заробітної плати розробників та працівників:

$$З_д = З_о \cdot 12 / 100\% ; \quad (5.4)$$

$$З_д = (27046,82 + 1898,44) \cdot 12 / 100\ \% = 3473,43 \text{ (грн.)}.$$

Нарахування на заробітну плату дослідників та працівників.

Згідно діючого законодавства нарахування на заробітну плату складають 22% від суми основної та додаткової заробітної плати:

$$Н_з = (З_о + З_д) \cdot * 22\% / 100\% ; \quad (5.5)$$

$$Н_з = (27046,82 + 1898,44 + 3473,43) * 22\% / 100\% = 7132,11 \text{ (грн.)}.$$

Витрати на матеріали на даному етапі проведення НДДКР пов'язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп'ютерної техніки та створення експериментального програмного забезпечення і системи захисту, тому дані витрати формуються на основі офісних витратних матеріалів.

Витрати на матеріали, що були використані при проведенні досліджень, розраховуються по кожному виду матеріалів за формулою [58]:

$$M = \sum_{1}^{n} H_i \cdot Ц_i \cdot К_i \quad , \quad (5.6)$$

де, - H_i - витрати матеріалу *і*-го найменування, кг;

$Ц_i$ - вартість матеріалу *і*-го найменування, грн./кг.;

$К_i$ - коефіцієнт транспортних витрат, $К_i = 1,1$;

n - кількість видів матеріалів,

Проведені розрахунки зводимо до табл. 5.3.

З врахуванням транспортних витрат вартість матеріалів складе

$$М = 4716,71 * 1,1 = 5188,38 \text{ грн.}$$

Витрати на комплектуючі (основне обладнання, емулятори), що були використані на дослідження підвищення інформаційної безпеки IP-телефонії, розраховуються за формулою:

$$Н = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i \quad , \quad (5.7)$$

де: *Нi* - кількість комплектуючих *i*-го виду, шт.;
Ці - покупна ціна комплектуючих *i*-го виду, грн.;
K_i - коефіцієнт транспортних витрат, $К_і$ = 1,1;
n - кількість видів матеріалів.

Таблиця 5.3 – Витрати на основні матеріали

Найменування матеріалу, марка, тип, сорт	Одиниця виміру	Ціна за одиницю, грн.	Витрачено	Вартість витраченого матеріалу, грн.
Папір офісний А4 білий (80%)	уп.	110,00	5,0	550,00
Диск оптичний (CD-R)	шт.	11,25	4,0	45,00
Органайзер офісний BOX-16A	уп.	89,00	6,0	534,00
Канцелярське приладдя	компл.	174,00	5,0	870,00
Тонер HP-26 (для заправки картриджа)	кг	6345,00	0,3180	2017,71
FLASH-пам’ять	шт.	350,00	2,0	700,00
Всього				4716,71

Проведені розрахунки зводимо до табл. 5.4.

Таблиця 5.4 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн.	Сума, грн.
Модуль підтримки цифрового потоку для IP-АТС Zycoo CooVox U50, U80 і U100	1	5600,00	5600,00
Escene ES410PE - IP-телефон	2	2940,00	5880,00
MikroTik - маршрутизатор	1	2240,00	2240,00
Escene ESH12 - професійна гарнітура для IP-телефонів і інтерфейсом RJ9 для підключення телефонної трубки	2	1120,00	2240,00
Всього			15960,00

Витрати на комплектуючі з урахуванням транспортних витрат складають:

$$H = 15960{,}00 \cdot 1{,}1 = 17556{,}00 \text{ (грн.)}.$$

Амортизація обладнання для проведення досліджень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню можуть бути розраховані з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12} \quad , \tag{5.8}$$

де $Ц_б$ – балансова вартість обладнання, приміщень тощо, які використовувались для розробки нового технічного рішення, грн.;

$t_{вик}$ – термін використання обладнання, приміщень під час розробки, місяців;

$T_в$ – строк корисного використання обладнання, приміщень тощо, років.

Проведені розрахунки необхідно звести до табл. 5.5.

Таблиця 5.5 - Величина амортизаційних відрахувань

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, міс.	Величина амортиза-ційних відрахувань, грн
Комп'ютеризований програмно-аналітичний комплекс	23800,00	5	1	396,67
CooVox EX16S - шістнадцятиканальний FXS шлюз з підтримкою VoIP і SIP Zyссo	9576,00	5	1	159,60
Програмне забезпечення підтримки IP-телефонії	30568,00	3	1	849,11
Місце оператора спеціалізоване	9780,00	5	1	163,00
Офісна оргтехніка	12300,00	4	1	256,25
Дослідницька лабораторія	215500,00	25	1	718,33
Всього				2542,96

Витрати на силову електроенергію на проведення досліджень розраховують за формулою [58]:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (5.9)$$

де, *В* – вартість 1 кВт-години електроенергії, *В* = 2,21 грн./кВт –година;

П – встановлена потужність обладнання, кВт.;

Ф – фактична кількість годин роботи обладнання, годин. ;

$К_п$ – коефіцієнт використання потужності.

Всі проведені розрахунки зведемо до табл. 5.6.

Таблиця 5.6 – Витрати на електроенергію при проведенні досліджень

Найменування обладнання	Кількість годин роботи обладнання, год.	Встановлена потужність, кВт	Коефіцієнт використання потужності	Величина оплати
Комп'ютеризований програмно-аналітичний комплекс	176,00	0,72	1	352,62
CooVox EX16S - шістнадцятиканальний FXS шлюз з підтримкою VoIP і SIP Zycco	105,00	0,02	1	5,66
Офісна оргтехніка	35,00	1,2	1	118,86
Місце оператора спеціалізоване	120,00	0,32	1	108,67
Всього				591,81

Інші витрати охоплюють: загальновиробничі витрати, адміністративні витрати, витрати на відрядження, матеріали, окремі непередбачені витрати, зв'язок, витрати на інтернет-послуги тощо.

Інші витрати доцільно приймати як 200...300% від суми основної заробітної плати дослідників та робітників. Величина інших витрат складе:

$$I = (27046,82 + 1898,44) * 200\% / 100\% = 57890,53 \text{ (грн.)}.$$

Загальні витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної та дослідно-конструкторської роботи:

$$В = 27046,82 + 1898,44 + 3473,43 + 7132,11 + 5188,38 + 17556,00 + 2542,96 + 591,81 + 57890,53 = 123320,48 \text{ (грн.)}.$$

5.2 Визначення коефіцієнта наукової значимості отриманих результатів науково-дослідної роботи

Коефіцієнт наукової значимості результатів проведеної НДР $K_{ЗН}$ можна підрахувати за формулою:

$$K_{ЗН} = \frac{\sum_{1}^{3} b_i \cdot d_i}{\sum_{1}^{3} b_{\max} \cdot d_i}, \qquad (5.10)$$

де b_i - значимість отриманих результатів: b_1 - ступінь наукової новизни, b_2 - рівень теоретичної обґрунтованості, b_3 - ступінь експериментальної перевірки результатів.

Таблиця 5.7 – Показники для оцінювання наукової значимості результатів виконання НДР

Характеристики	Питома вага характеристик	Бальна оцінка характеристик		
		Ступінь новизни b_1	Рівень теоретичної обґрунтованості b_2	Ступінь експериментальної перевірки результатів b_3
		1	3…5	7…10
b_1	0,500	Часткове удосконалення виробів, технологій, матеріалів, програмного продукту, тощо	Суттєве удосконалення виробів, технологій, матеріалів, програмного продукту, тощо	Нові напрямки в розробці виробів, технологій, матеріалів, програмного продукту, тощо. Створення принципово нової техніки
b_2	0,333	Позитивне рішення на основі зроблених узагальнень	Установлення залежностей, які використовувались в інших випадках	Відкриття нових шляхів рішення задачі
b_3	0,167	Експериментальна перевірка не робилась	Результати перевірялись на невеликій кількості даних	Результати перевірені на великій кількості даних

Максимальне значення отриманих результатів можна прийняти в межах 7…10 балів; d_i - питома вага кожної характеристики, значення якої наведено

в табл. 5.7; З – кількість характеристик, за якими була зроблена оцінка результатів науково-дослідної роботи.

Підставляючи числові дані $d_1 = 0{,}5$, $d_2 = 0{,}333$, $d_3 = 0{,}167$, $b_{\max} = 10$ у вираз (5.10) оцінимо наукову значимість отриманих результатів:

$$K_{ЗН} = \frac{7 \cdot 0{,}5 + 6 \cdot 0{,}333 + 6 \cdot 0{,}167}{10 \cdot 0{,}5 + 10 \cdot 0{,}333 + 10 \cdot 0{,}167} = 0{,}65.$$

5.3 Внесок дослідника в досягнення отриманих результатів НДР

Внесок дослідника в досягнення отриманих результатів НДР можна розрахувати за формулою:

$$V = \frac{k_{TBI} \cdot З_i}{\sum_{1}^{n} k_{TBI} \cdot З_i}, \qquad (5.11)$$

де k_{TBI} - коефіцієнт творчої участі кожного виконавця НДР, який оцінюється наступним чином: проведення досліджень – 3 бали, робоче проектування – 1,5 бали, освоєння – 1,0 балів.

Якщо виконавець приймав участь в декількох видах робіт, то береться сума відповідних балів;

$З_i$ - заробітна плата кожного виконавця НДР;

n - кількість всіх виконавців НДР,

Розраховуємо внесок дослідника:

$$V = \frac{3 \cdot 10100{,}00}{3 \cdot 10100{,}00 + 3 \cdot 9570{,}00 + 1{,}5 \cdot 11540{,}00} = 0{,}46.$$

5.4 Висновки до розділу 5

Загалом запланована науково-дослідна робота з дослідження підвищення інформаційної безпеки IP-телефонії вимагає вкладення для проведення досліджень в межах 123320,00 грн.

Отримані результати досліджень мають високий рівень наукової значимості (в межах 0,65), що свідчить про доцільність проведення розробок.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Мета реалізації системи управління охороною праці – це всебічне сприяння виконанню вимог, що цілком ліквідують, нейтралізують чи зменшують до допустимих норм вплив на працівників шкідливих і небезпечних факторів виробничого середовища, створюють безпечні ергономічні та санітарно-гігієнічні вимоги. В даному розділі наводиться розгляд шкідливих, небезпечних і уражаючих для людини і навколишнього середовища чинників, що виникають під час проведення удосконалення інформаційної безпеки IP-телефонії. В ньому розглядаються, в тому числі, технічні рішення з виробничої санітарії та гігієни праці, визначення ефективності екрану для захисту від шуму, технічні рішення з промислової та пожежної безпеки при проведенні удосконалення, безпека в надзвичайних ситуаціях.

Під час удосконалення вказаного пристрою на працівників вливають ті чи інші небезпечні і шкідливі виробничі фактори (НШВФ) фізичної та психофізіологічної груп відповідно до [60]. Фізичні небезпечні і шкідливі виробничі фактори: понижена або підвищена температура повітря робочої зони, підвищений рівень шуму на робочому місці, підвищений рівень статичної електрики, недостатність або відсутність природного освітлення, недостатня освітленість робочої зони, підвищена яскравість світла, відбита або пряма блискучість. Психофізіологічні небезпечні і шкідливі виробничі фактори: нервово-психічні перевантаження: розумове перенапруження, монотонність праці, перенапруження аналізаторів.

6.1 Гігієна праці та виробнича санітарія

6.1.1 Склад повітря робочої зони та мікроклімат

Визначаємо для приміщення, в якому проводяться роботи з удосконалення інформаційної безпеки IP-телефонії, категорію важкості робіт за фізичним навантаженням – легка Іа.

Відповідно до [61] допустимі параметри температури, відносної вологості та швидкості руху повітря у робочій зоні для теплого та холодного періодів року приведені у табл. Х.1 додатку Х.

Розкид значень температури повітря за висотою робочої зони для всіх категорій робіт допускається до 3°С. Для опромінення менше 25% поверхні тіла людини, нормована інтенсивність теплового опромінення сладає 100 Вт/м^2.

Повітря робочої зони не повинно містити шкідливих речовин з концентраціями вище гранично допустимих концентрацій (ГДК), що використовуються при проектуванні виробничих приміщень (будівель), обладнання, технологічних процесів, вентиляцій, з метою контролю за якістю виробничого середовища. ГДК шкідливих речовин, які використовуються в даному виробничому приміщені наведено в табл. Х.2 додатку Х.

З метою забезпечення необхідних за нормативами показників мікроклімату та чистоти повітря робочої зони запропоновано такі заходи:

1) у приміщенні повинна бути розміщена система кондиціонування для теплого і опалення для холодного періодів року;

2) щоденне вологе прибирання;

3) застосування витяжної вентиляції, яка видаляє забруднення або нагріте повітря з приміщення, а також за допомогою неї контролюється швидкість руху повітря і вологість.

6.1.2 Виробниче освітлення

З метою забезпечення гігієнічних раціональних умов на робочих місцях значні вимоги пред'являються щодо кількісних та якісних параметрів освітлення.

З погляду задач зорової роботи в приміщенні, в якому проводяться роботи з удосконалення інформаційної безпеки IP-телефонії, відповідно до [3] визначаємо, що вони відповідають III розряду зорових робіт. Приймаємо контраст об'єкта з фоном – середній, а характеристику фону – середню, яким відповідає підрозряд *в*.

Нормативні значення коефіцієнта природного освітлення (КПО) та мінімальні значення освітленості для штучного освітлення приведені в табл. Х.3 додатку Х.

Оскільки приміщення розташоване в місті Вінниця (друга група забезпеченості природним світлом), а вікна орієнтовані за азимутом 0°, то за таких умов КЕО визначатиметься за виразом [62, 63]

$$e_N = e_н m_N \ [\%], \qquad (6.1)$$

де $e_н$ – табличне значення КЕО, %;

m_N – коефіцієнт світлового клімату;

N – порядковий номер групи забезпеченості природним світлом.

Підставляючи відомі значення одержимо нормовані значення КПО для бокового та суміщеного освітлення:

$$e_{N.б} = 2 \cdot 0,9 = 1,8\ (\%);$$

$$e_{N.с} = 1,2 \cdot 0,9 = 1,1\ (\%).$$

З метою забезпечення нормованих значень показників освітлення запропоновано такі заходи:

1) при недостатньому природному освітлені в світлу пору доби доповнення штучним завдяки використанню газорозрядних ламп з утворенням системи суміщеного освітлення;

2) використання штучного освітлення в темну пору доби.

6.1.3 Виробничі віброакустичні коливання

Зважаючи на те, що при експлуатації пристроїв крім усього іншого устаткування використовується обладнання, робота якого генерує шум та вібрацію, потрібно передбачити шумовий та вібраційний захист.

Визначено, що приміщення, де проводиться робота з удосконалення інформаційної безпеки IP-телефонії може мати робочі місця із шумом та вібрацією, який поширюється від сусідніх виробничих приміщень.

З метою попередження травмування працюючих під дією шуму та вібрації вони підпадає під нормування. Основним нормативом з питань виробничого шуму, діючим в нашій країні, є [64], згідно з яким допустимі рівні звукового тиску, рівні звуку і еквівалентні рівні шуму на робочих місцях у виробничих приміщеннях не мають бути більшими ніж значення, які наведено у табл. Х.4 додатку Х. Норми виробничих вібрацій наведені в табл. Х.5 додатку Х для 3-ї категорії (технологічна) типу "в".

З метою поліпшення віброакустичного клімату в приміщенні передбачено такі заходи:

1) своєчасне здійснення профілактичного ремонту;

2) використання в конструкціях обладнання віброізоляції та акустичних екранів.

Вихідні дані: розмір сторони екрану H = 1,9 м, відстань від джерела шуму до екрану R = 0,5 м, відстань від екрану до працівника D = 0,7 м, частота шуму f = 14 кГц.

Для визначення послаблення шуму треба знайти спочатку величину N

$$N = \frac{2}{\lambda}\left[R\left(\sqrt{1+\left(\frac{H}{R}\right)^2} - 1\right) + D\left(\sqrt{1+\left(\frac{H}{D}\right)^2} - 1\right)\right] \quad , \qquad (6.2)$$

де λ – довжина хвилі, м;

R – відстань від джерела шуму до екрану, м;

D – відстань від екрану до працівника, м;

H – розмір сторони екрану, м.

Довжину хвилі можна визначити за формулою

$$\lambda = \frac{c}{f} \quad [\text{м}], \qquad (6.3)$$

де c – швидкість звуку в повітрі за нормальних умов, м/с (c = 330 м/с); f – частота коливань, Гц.

Підставляючи відомі значення у формули (5.3, 5.2) отримаємо

$$\lambda = \frac{330}{14 \cdot 10^3} = 0{,}023571 \text{ (м)};$$

$$N = \frac{2}{0{,}023571}\left[0{,}5\left(\sqrt{1+\left(\frac{1{,}9}{0{,}5}\right)^2} - 1\right) + 0{,}7\left(\sqrt{1+\left(\frac{1{,}9}{0{,}7}\right)^2} - 1\right)\right] = 236{,}69203.$$

За величиною N = 236,69203 вибираємо послаблення шуму L = 21,829 дБ.

6.1.4 Виробничі випромінювання

Проведений аналіз умов праці показав, що приміщення, в якому виконується робота з удосконалення інформаційної безпеки IP-телефонії може містити електромагнітні випромінювання.

Гранично допустимі рівні електромагнітних полів наведені у табл. Х.6 додатку Х.

Для гарантування захисту та досягнення нормованих рівнів випромінювань необхідно застосовувати екранні фільтри та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

6.2 Технічні рішення з промислової та пожежної безпеки при проведенні удосконалення інформаційної безпеки IP-телефонії

6.2.1 Безпека щодо організації робочих місць

Конструкція робочого місця, взаємне розташування його елементів та його розміри повинні відповідати антропометричним, психофізіологічним і фізіологічним властивостям працівника, а також характеру роботи [66].

Площа, на якій розташовується одне робоче місце для обслуговуючого персоналу, має становити не менше 6,0 м^2, об'єм приміщення – не менше ніж 20 м^3, висота – не менше 3,2 м [67].

Інтер’єр приміщень потрібно оздоблювати дифузно-віддзеркалювальними матеріалами з коефіцієнтом відбиття: стелі 0,7-0,8; стін 0,4-0,5; підлоги 0,2-0,3. Поверхня підлоги має бути гладкою, без вибоїн, не слизькою, мати антистатичні властивості, зручною для вологого прибирання. Забороняється застосовувати під час оснащення інтер'єру полімери, які забруднюють повітря шкідливими хімічними речовинами та сполуками.

6.2.2 Електробезпека

Основними причинами ураження електричним струмом в даному приміщенні можуть бути: робота під напругою під час проведення ремонтних робіт, несправність устаткування, випадкове торкання до металевих частин, які опинилися під напругою або струмоведучих частин. У відповідності до [68] це приміщення відноситься до приміщень із підвищеною небезпекою ураження електричним струмом в наслідок наявності високої (більше 75 %) відносної вологості. Через це безпека експлуатації електрообладнання повинна забезпечуватись комплексом заходів, які включають використання ізоляції струмовідних частин, захисного заземлення, захисних блокувань та ін [69].

6.2.3 Пожежна безпека

Згідно [70] приміщення, в якому проводиться робота з удосконалення інформаційної безпеки IP-телефонії, відноситься до категорії пожежної небезпеки Б. Дане приміщення відноситься до 2-го ступеня вогнестійкості, в

якому приміщення знаходяться в будівлі з несучими та огороджувальними конструкціями з природних або штучних кам'яних матеріалів, бетону, залізобетону із застосуванням листових і плитних негорючих матеріалів.

Мінімальні межі вогнестійкості конструкцій приміщення, що розглядається наведені в табл. Х.7. В табл. Х.8 приведено протипожежні норми проектування будівель і споруд.

Встановлюємо, що приміщення, де проводиться робота з удосконалення, має бути оснащене двома вогнегасниками, пожежним щитом, ємністю з піском [61].

6.3 Безпека в надзвичайних ситуаціях

6.3.1 Визначення області працездатності мережі IP-телефонії в умовах дії загрозливих чинників надзвичайних ситуацій

Вплив іонізуючих випромінювань (α, β, γ) на матеріал і деталі обладнання залежить від виду випромінювання, дози та умов навколишнього середовища. В РЕА застосовуються елементи, до складу яких входять такі матеріали: метали, неорганічні матеріали (в основному діелектрики), провідники і різноманітні органічні сполуки (діелектрики, смоли і т.д.).

В радіоелектронній апаратурі іонізуючі випромінювання, викликають зворотні і незворотні процеси, внаслідок яких можуть відбуватися порушення роботи електричних елементів схеми, що призводять до виходу з ладу апаратури. Так, проходячи через елементи РЕА, потік гамма-випромінень створює в них вільні носії електричних зарядів, в результаті переміщення яких виникає помилковий імпульс, який призводить до спрацьовування пристрою. При великих дозах випромінювання втрачають працездатність комплектуючі елементи систем радіоелектроніки і електроавтоматики. У органічних ізоляційних і діелектричних матеріалах змінюються такі параметри, як: електрична провідність, діелектрична проникність і тангенс кута втрат. Неорганічні матеріали менш чутливі до впливу іонізуючих випромінювань [63].

Для інженерної практики найбільший інтерес представляє перший випадок, тобто оцінка стійкості роботи РЕА при перебуванні її в зараженій радіоактивними речовинами місцевості протягом еталонного часу.

Найбільш піддаються впливу електромагнітних випромінювань (EMI) системи електропостачання, зв'язку, сигналізації і керування. EMI ушкоджують напівпровідникові прилади, резистори, конденсатори. Також EMI представляє велику небезпеку для апаратури, добре захищеної від впливу

інших вражаючих факторів. Слід пам'ятати про те, що захист апаратури від механічних ушкоджень не захищає від впливу ЕМІ. Прилад може втратити працездатність, знаходячись у надійних захисних спорудженнях [25].

6.3.2 Визначення області працездатності мережі IP-телефонії в умовах дії іонізуючих випромінювань

Вихідні дані коефіцієнт послаблення $К_{посл}=2$

Приймаючи до уваги елементну базу, що використовується для реалізації розроблювального пристрою, складається таблиця потужностей експозиційної дози опромінення для кожного елемента $Р_{зв.і}$, що викликають початок зворотних змін (табл. 6.1).

Таблиця 6.1 – Потужність експозиційної дози для елементів пристрою.

Елементи радіоелектронної схеми	$Р_{зв.і}$, Р/с	$Р_{зв.}$, Р/с
Фотоелементи	10^3	10^3
Діоди загального призначення	10^4	
Транзистори загального призначення	10^4	
Мікросхеми	10^5	
Конденсатори	10^7	
Резистори	10^8	

Визначається елемент, який найбільшою мірою піддається впливу випромінюванням, тобто елемент із мінімальним значенням $Р_{зв}$. $Р_{зв} = 10^3$ Р/с.

В якості критерію стійкості роботи пристрою використовується граничне значення рівня іонізуючих випромінювань:

$$Р_{гр} = К_{над*} Р_{зв*} К_{посл}.$$

де $Р_{зв}$ - рівень радіації, який відповідає початку зворотних змін у найбільш беззахисного елемента схеми;

$К_{над}$ - коефіцієнт надійності ($К_{над}$ =0,9÷0,96);

$К_{посл}$ - коефіцієнт послаблення.

$Р_{гр} = 0,96* 10^3 *2 = 1920$ Р/с.

Отже, електричні кола розроблювальної мережі будуть працювати з потрібною якістю в області зміни потужності дози від 0 до $1,92*10^3$Р/с.

6.3.3 Визначення області працездатності мережі IP-телефонії в умовах дії електромагнітного імпульсу

В якості показника стійкості електротехнічних і електронних систем або їх окремих елементів до впливу ЕМІ можна прийняти коефіцієнт безпеки, що визначається відношенням гранично допустимої напруги (струму) до наведеної, тобто створеної ЕМІ в даних умовах :

$$K_{Б} = 20lg\frac{Uд}{Uв(г)} \geq 40дБ,$$

Де $U_д$ - допустиме коливання напруги живлення (в даному пристрої для його використовується напруга $U_ж$ = 5 В ±5% (N=5));

$U_{в/г}$ - напруга наведена за рахунок електромагнітного імпульсу у вертикальних (горизонтальних) струмопровідних частинах.

Апаратура працює стійко, коли $К_Б$ > 40 дБ.

Допустиме коливання напруги живлення визначається за формулою:

$$U_д = U_ж + \frac{U_ж}{100} * N = 5 + \frac{5}{100} = 5.25(B)\,.$$

Визначається напруга наведення у горизонтальних провідниках $U_г$:

$$U_г = \frac{Uд}{10^{\frac{40}{20}}} = \frac{150}{100} = 1,5(B).$$

Тоді вертикальна складова напруженості електричного поля визначається з виразу:

$$U_г=E_в*L_г;$$

$$E_г=U_г/ L_г =1,5/0,51=2,12В/м,$$

де: $I_в$ - максимальна довжина струмопровідної частини $l_в$= 0,51 м.

Отже, при умові, що $E_г \leq 2,12$ В/м мережі IP-телефонії можлива.

6.3.4 Розробка заходів по підвищенню безпеки роботи мережі IP-телефонії в умовах дії електромагнітного імпульсу

Дослідження, які були проведені як у нашій країні, так і за кордоном, показали, що зміна параметрів радіоелектронних пристроїв може відбуватися в широкому діапазоні доз (потоків) іонізуючих випромінювань. Тому в багатьох випадках виникає необхідність вживати заходів по підвищенню радіаційної стійкості розроблювальної апаратури (пристроїв, блоків).

Головними заходами щодо підвищення радіаційної стійкості являються: застосування в апаратурі радіаційностійких елементів і матеріалів, спеціальних масивних екранів або активного захисту від впливу потоків заряджених частинок. При імпульсному впливі іонізуючих випромінювань, крім перерахованих способів використовують: застосування схем, мало критичних до змін електричних параметрів; зниження напруги живлення на аноді і збільшення від'ємної напруги зсуву сіток газорозрядних приладів; застосування пристроїв, які містять радіотехнічні схеми на період впливу радіації; збільшення відстані між елементами, які знаходяться під навантаженням і інші.

6.4 Висновки до розділу 6

Під час виконання цього розділу було опрацьовано такі питання охорони праці і безпеки в надзвичайних ситуаціях, як технічні рішення з гігієни праці та виробничої санітарії, визначення ефективності екрану для захисту від шуму, технічні рішення з промислової та пожежної безпеки при проведенні удосконалення інформаційної безпеки IP-телефонії, безпека в надзвичайних ситуаціях.

Також було проведено визначення області працездатності мережі IP-телефонії в умовах дії іонізуючих випромінювань та електромагнітного імпульсу. Аналізуючи вищенаведені розрахунки, можна зробити висновок, що електричні кола розроблювального пристрою будуть зберігати працездатність при рівні іонізуючих випромінювань меншому $1{,}92 * 10^3$ Р/с.

При визначенні області працездатності електротехнічних і електронних систем було визначено, що безпека роботи розроблювального мережі IP-телефонії можлива при умові $Ев \leq 2{,}12$В/м.

ВИСНОВОК

У МКР вирішена актуальна науково-технічна задача підвищення рівня захищеності інформації в сеансах безпечної IP- телефонії та скорочення часу встановлення захищеного з'єднання за рахунок поліпшення ймовірносно-часових характеристик протоколів, в тому числі отримані наступні основні результати:

1. Запропоновано математичну модель активного порушника для захищеної IP-телефонії, що враховує можливість цього порушника реалізувати атаку людина посередині на протокол розподілу ключів, яка дозволяє розрахувати ймовірність успішної атаки, націленої на несанкціонований доступ до інформації (НСД), в залежності від значень ймовірностей проміжних атак .

2. Запропоновано методику оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії, що враховує особливості протоколів, виражені в наявності обмеження числа повторних передач повідомлень і змінного таймера повторної передачі.

3. Представлена модифікація протоколу розподілу ключів ZRTP, яка дозволяє виконувати протокол за менший час у порівнянні з вихідною реалізацією. Виграш досягається за рахунок поліпшення тимчасових характеристик протоколу розподілу ключів ZRTP, що складається у виключенні алгоритму розподілу ролей ініціатора і респондента, а також в об'єднанні інформаційних даних про підтримуваних криптографічних наборах і блоків протоколу Діффі - Хелмана.

4. Розроблено метод виявлення порушника протоколів розподілу ключів, який застосовується при роботі за сценарієм клієнт-клієнт для кореспондентів, які не мають заздалегідь розподіленого ключового матеріалу. Метод дозволять з більш високою ймовірністю встановити захищене з'єднання між двома кореспондентами в порівнянні з існуючими методами, а також виявити наявність активного порушника в каналі зв'язку.

5. Запропоновано модифікації протоколу ZRTP, що реалізують розроблений метод виявлення порушника. Модифікації в порівнянні з вихідним протоколом дозволяють з виявити активного порушника, що реалізує атаку людина посередині на протокол розподілу ключів.

Перспективними завданнями дослідження є розробка програмної реалізації модифікованого протоколу розподілу ключів із застосуванням загальнодоступних бібліотек, розробка програмного клієнта IP-телефонії, що реалізує протокол, а також доопрацювання рішення за рахунок впровадження елементів стеганографії в пропоновані метод підвищення безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Докучаев В.А. Защита информации на корпоративных сетях VoIP / В.А. Докучаев, А.В. Шведов // Электросвязь. –2012. –№ 4.– с. 5–8. Макарова О. С. Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» / О. С. Макарова // Докл. Томского государственного университета систем управления и радиоэлектроники. –2012.–№ 1. с. 51–67.

2. Атрощенко В.А. К вопросу оценки достоверности информации для предотвращения MITM-атаки при передаче закрытой информации по открытым каналам связи / Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Багдасарян Р.Х. //Современные проблемы науки и образования. –2013– №. 3. – с. 82-88.

3. Радивилова, Т.А., Анализ основных атак на dns-сервер и методы использования DNSSec при защите DNS-сервера / Т.А. Радивилова, В.С. Бушманов // Технологический аудит и резервы производства. –2013– Т. 2. № 1 (10).– С. 16-19.

4. Карпухин, Е.О., Метод формирования сетевых пакетов для защиты от информационных атак «человек посередине» в телекоммуникационных сетях / Е.О. Карпухин, В.Ю. Михайлов // Вопросы радиоэлектроники. – 2013– Т. 3. № 2. – С. 83-93.

5. Мошак, Н.Н. Модель сигнального трафика в защищенной мультисервисной сети / Н.Н. Мошак, С.Р. Рудинская// XVIII международная научно-техническая конференция «Современные средства связи». Минск, 15-16 октября 2013 г.: Материалы конференции / Высший государственный колледж связи. – г. Минск, 2013. – С. 45-47

6. Федосеева, О.С. "Исследование особенностей обеспечения характеристик качества обслуживания различных типов трафика в NGN-мультисервисных сетях" [Електронний ресурс]. – 2019. –Режим доступу: http://masters.donntu.edu.ua/2007/kita/fedoseeva/diss/diss.htm

7. E. Gelenbe Cognitive Packet Networks: QoS and Performance / E. Gelenbe, R. Lent, A. Montuori , Z. Xu // School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816 [Електронний ресурс]. – 2019. – Режим доступу: http://pdf.aminer.org/000/339/717/cognitive_routing_in_packet_networks.pdf (Дата обращения: 22.04.2014)

8. Д. В. Юркин, А. В. Винель, В. В. Таранин Анализ временных и сложностных характеристик парольной аутентификации в защищенных

операционных системах семейства UNIX // Информационно-управляющие системы - № 3 (64) - 2013 - С. 62 - 66.

9. Миронова, В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информационная безопасность систем. – 2012. – № 1. с. 28-35.

10. Десницкий, В. А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами/ Десницкий В. А., Чеулин А. А. // Технические науки — от теории к практике. Сб. ст. по материалам XXXIX междунар. науч.-практ. конф. – Новосибирск: Издательство СибАК – 2014. – №10(35) – С. 7-20

11. Бахметьев, Б. Безопасность VoIP-соединений / Бахметьев Б. // Первая миля. - 2014. - № 2 (41). - С. 88-93.

12. Балашов, Д. Безопасность Vo P / Балашов Д. // Технологии и средства связи. - 2013. - № 4 (97). - С. 38-40. Синюк, А.Д. Математическая модель нарушителя открытого ключевого согласования сети с минимальным числом корреспондентов/А.Д. Синюк, О.А. Остроумов //Наукоемкие технологии в космических исследованиях Земли. - 2013. - Т. 5. № 1.- С. 20-24

13. Шабуров, А.С. Моделирование оценки угроз безопасности информационных систем персональных данных/А.С. Шабуров, С.А. Юшкова, А.В. Бодерко // Вестник ПНИПУ. – 2013. – № 7. С. 149–159.

14. Глотов, В. Правовые вопросы рынка VoIP / Глотов В. // Первая миля. - 2014. - № 2 (41). - С. 118-120.

15. Ковцур М.М. Оценка скоростных характеристик реализации атаки типа перебор пароля на IP-АТС при использовании FAIL2BAN / М.М. Ковцур, А.А. Молдовян// Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015. – 418 с. – С. 171

16. Рекомендация ITU-T Y.1541(12/2011) Требования к сетевым показателям качества для служб, основанных на протоколе IP [Електронний ресурс]. – 2019. –Режим доступу: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11462&lang=ru

17. Comer, D. Internetworking With TCP/IP Vol I:Principles, Protocols, and Architecture/ D. Comer. – New Jersey: Pearson Education, Inc.,2014. – 698 p.

18. Григорьев, В. А. Анализ пропускной способности сети радиосвязи стандарта IEEE 1609 / Григорьев В.А., Никитин В.Н., Кузнецов В.И., Тараканов С.А., Ковцур М.М. //Электросвязь.–2014– №.1.–с. 10-12

19. Рекомендация ITU-T G.107 (02/2014) The E-model: a computational model for use in transmission planning [Електронний ресурс]. – 2019. – Режим доступу: http://www.itu.int/rec/T-REC-G.107

20. Каримжанова А.С. Исследование возможности улучшения качества предоставления услуг в мультисервисных сетях передачи: пояснительная записка к магистерской диссертации по специальности 6М071900, Некоммерческое акционерное общество «Алматинский университет энергетики и связи», Алматы 2013 [Електронний ресурс]. – 2019. – Режим доступу: http://www.aipet.kz/student/mag_disser/2013/karimzhanova _ainur.pdf

21. Малаховский, А.А. Организация мультимедийной связи в сетях с низкоскоросными и нестабильными каналами связи / А.А. Малаховский, Н.И. Лычагин, А.С. Гузарев // Техника средств связи: Научно-технический сб. – №1 (140). – СПб: Политехнический университет, 2012. С 88-95

22. Ковцур, М. М. Протоколы обеспечения безопасности VoIP-телефонии/ М. М. Ковцур , В. Н. Никитин, Д. В. Юркин // Защита информации. Инсайд. – 2012. – №3. – с. 74-81.

23. Никитин, В.Н. Обеспечение информационной безопасности ИТС /Никитин В.Н., Лагутенко О.И., Ковцур М.М. //Электросвязь.–2014– №.1.–с. 29-31

24. Ковцур, М.М. Протоколы обеспечения безопасности IP-телефонии. / М.М. Ковцур // Первая миля. – 2012. – №5. – С.18-26.

25. Привалов, А.А. Модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя /Привалов А.А., Евглевская Н.В., Зубков К.Н. // Известия петербургского университета путей сообщения. -2014 -№2 (39).- С. 106-111

26. Ковцур М.М. Исследование путей совершенствования протоколов распределения ключей в защищенной IP-телефонии / М.М. Ковцур//Фундаментальные исследования. – 2014 – № 8(часть 6). – С. 1300-1308.

27. Статистика уязвимостей корпоративных информационных систем (2013 год) [Електронний ресурс]. – 2019. – Режим доступу: http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2014_rus.pdf

28. PGPfone Pretty Good Privacy Phone Owner’s Manual ,Version 1.0 beta 7 -8 July 1996 Philip R. Zimmermann [Електронний ресурс]. – 2019. – Режим доступу: ftp://ftp.pgpi.org/pub/pgp/pgpfone/manual/pgpfone10b7.pdf

29. АНБ занимается экономическим шпионажем [Електронний ресурс]. – 2019. – Режим доступу: http://www.securitylab.ru/news/444645.php/

30. Facebook не может защитить пользователей от MITM-атак [Електронний ресурс]. – 2019. – Режим доступу: http://www.securitylab.ru/news/450391.php /

31. Wi-Fi spies - 34% use no protection at Wi-Fi hot spots [Електронний ресурс]. – 2019. – Режим доступу: http://www.kaspersky.com/about/news /press/2013/Wi-Fi_spies_-_34_percent_use_no_protection_at_Wi-Fi_hot_spots / (дата обращения: 01.05.13).

32. Таргетированные MiTM-атаки с перенаправлением интернет-трафика по BGP [Електронний ресурс]. – 2019. – Режим доступу: http://www.xakep.ru/post/61620/default.asp

33. Ковцур М.М. Математическая модель активного нарушителя для защищенной IP-телефонии / М.М. Ковцур, В.Н. Никитин // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно - методическая конференция: сб. научных статей в 2 т. / под. ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. - СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. - 920 с. С 330-335

34. Advanced Encryption Standard [Електронний ресурс]. – 2019. – Режим доступу: http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard#cite _note-19

35. В.Н. Пути совершенствования протоколов распределения ключей для IP-телефонии / В.Н. Никитин, М.М. Ковцур // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II-я Международная научно-техническая конференция: сб. научных статей / под. ред. С.М. Доценко, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. - СПб.: Санкт- Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2013. С 852 – 855

36. Коржик, В.И. Основы криптографии/В.И. Коржик, В.П. Просихин, В.А.Яковлев - СПб.: СПбГУТ, 2014. - 276 с.

37. Лобашев, А.И. Защита сигнально-управляющего трафика стохастическими методами /А.И. Лобашев А.И., С.В. Баранов С.В., И.В. Симоненко И.В., Е.В. Шалашов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. - 2015. - № 3-4.- С. 32-34.

38. Демьянчук А.А. Способ повышения уровня безопасности протоколов аутентификации с нулевым разглашением секрета/ А.А. Демьянчук , Е.С. Новикова, Д.Н. Молдовян// Материалы VIII СПб межрегион. конф.«Информационная безопасность регионов России (ИБРР-2013)».- Спб.:ООО «К-8» - 2013 - С. 51-52.

39. C++ Implementation of ZRTP protocol - GNU ZRTP C++ [Електронний ресурс]. – 2019. – Режим доступу: https://github.com/wernerd /ZRTPCPP

40. ZRTP Protocol Library [Електронний ресурс]. – 2019. – Режим доступу: http://freecode.com/projects/libzrtpcpp

41. Кипчатов А. Введение в индустрию интернет : структура провайдинга [Електронний ресурс]. – 2019. – Режим доступу: http://nag.ru/articles/reviews/15477/vvedenie-v-industriyu-interneta-struktura-provaydinga.html

42. Tier 1 network Definition from PC Magazine Encyclopedia [Електронний ресурс]. – 2019. – Режим доступу: http://www.pcmag.com/encyclopedia/term/60763/tier- 1-network

43. Tier-1-операторы [Електронний ресурс]. – 2019. – Режим доступу: http://ru.wikipedia.org/wiki/Tier-1-операторы

44. The Cooperative Association for Internet Data Analysis [Електронний ресурс]. – 2019. – Режим доступу: http://as-rank.caida.org/

45. S Rank: AS 12389 OJSC Rostelecom -- AS Relationship Graph - CAIDA : http://as-rank.caida.org [Електронний ресурс]. – 2019. – Режим доступу: http://as- rank.caida.org/?mode0=as-info&mode1=as-graph&as=12389

46. Ковцур, М.М. Исследование непересекающихся маршрутов глобальной сети / Ковцур М.М. // VI международная научно-практическая конференция "Наука вчера, сегодня, завтра." №6. материалы конф. – Новосибирск:Издательство СибАК – 2013. – С. 19-24.

47. Geo IP Tool [Електронний ресурс]. – 2019. – Режим доступу: http://www.geoiptool.com/

48. Липатников, В.А. Метод многоуровневой проактивной информационной безопасности компьютерной сети / Липатников В.А., Костарев С.В., Корольков А.П. // Проблемы управления рисками в техносфере.– 2014.– № 1 (29) – С. 81- 89.

49. Ковцур, М.М. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи / М. М. Ковцур, В.Н. Никитин, Д. В. Юркин // Информационно–управляющие системы. – 2014. – №1(68) – С. 70-75.

50. Ковцур, М.М. Исследование вероятностно-временных характеристик протокола распределения ключей защищенной IP-телефонии / М.М. Ковцур, В.Н. Никитин, А.В. Винель // Информационно – управляющие системы. –2013.– №1(62). –С. 54-63.

51. Красов, А.В., О вероятностно-временных характеристиках синхронизации систем передачи с широкополосными сигналами / А.В. Красов, М.М. Ковцур, В.Н. Никитин //Труды конференции Телекоммуникационные и

вычислительные системы, 28 ноября 2012 г.–М.: Московский технический университет связи и информатики, 2012. – с. 142

52. Ковцур, М.М. Исследование ВВХ протоколов обеспечения безопасности VoIP телефонии при работе по каналам связи с ошибками. / М.М. Ковцур // Международная научно-техническая и научно-методическая конференции "Актуальные проблемы инфотелекоммуникаций в науке и образовании" №64.: материалы конф. – СПб.: Издательство СПбГУТ, 2012. – С. 235 - 236.

53. Ковцур, М. М. Оценка вероятностно-временных характеристик защищенной IP-телефонии / М. М. Ковцур, В. Н. Никитин // Защита информации. Инсайд. – 2012. №4. – С. 38-44.

54. RFC6347 (01/2012) Datagram Transport Layer Security Version 1.2 [Електронний ресурс]. – 2019. – Режим доступу: http://tools.ietf.org/html/rfc6347

55. RFC 6298 - Computing TCP\x27s Retransmission Timer RFC6298 [Електронний ресурс]. – 2019. – Режим доступу: https://tools.ietf.org/html/rfc6298

56. Ковцур, М.М. Экспериментальная оценка временных характеристик протокола ZRTP / М.М. Ковцур, В.Н. Никитин // сборник материалов всероссийской конференция «Современные экономические информационные системы: актуальные вопросы организации, методы и технологии защиты информации» / Межрегиональный открытый социальный институт (МОСИ). – Йошкар-Ола. – 2012. –С. 30–35.

57. Ковцур, М.М. Оптимизация вероятностно-временных характеристик криптографического протокола распределения ключей IP-телефонии / М.М. Ковцур // Universum: технические науки. – 2014. – № 2 (3). – С. 1-9.

58. Методичні вказівки до виконання студентами-магістрантами наукового напрямку економічної частини магістерських кваліфікаційних робіт / Уклад. В.О. Козловський – Вінниця: ВНТУ, 2012. – 22 с.

59. Козловський В.О. Техніко-економічні обґрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – Вінниця : ВДТУ, 2003. – 75с.

60. ГОСТ 12.0.003-74.ССБТ. Опасные и вредные производственные факторы. Классификация.

61. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.

62. ДБН В.2.5-28-2006. Природне і штучне освітлення.

63. Пособие по расчету и проектированию, естественного, искусственного и совмещенного освещения НИИСФ – М.: Стройиздат. 1985. – 384 с.

64. ДСН 3.3.6-037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

65. ДСН 3.3.6.039-99. Державні санітарні норми виробничої та загальної вібрацій.

66. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.

67. Методичні вказівки до опрацювання розділу "Охорона праці та безпека в надзвичайних ситуаціях" в дипломних проектах і роботах студентів спеціальностей, що пов’язані з функціональною електронікою, автоматизацією та управлінням / Уклад. О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2012. – 64 с.

68. Правила улаштування електроустановок. 2-е вид., перероб. і доп. – Х: "Форт", 2009. – 736 с.

69. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.

70. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.

71. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.

72. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.

73. Норми радіаційної безпеки України (НРБУ-97), МОЗ України. – К., 1997.

ДОДАТКИ

Додаток А
(обов’язковий)

Технічне завдання

Додаток Б
(обов’язковий)

Принципова схема підключення оператора VoIP

Додаток В
(обов’язковий)

Архітектурна модель для підтримки QoS

Додаток Г
(обов’язковий)

Структурна схема з'єднання в сценарії клієнт-клієнт

Додаток Д
(обов’язковий)

Алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником

Додаток Е
(обов’язковий)

Алгоритм дій при захопленні терміналу користувача зовнішнім порушником

Додаток Є
(обов’язковий)

Алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником

Додаток Ж
(обов’язковий)

Алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником

Додаток А

(обов'язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ ВНТУ,

канд. техн. наук, професор

Г.Г.Бортник

. "__" _____ 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

08-34.МКР.001.00.000 ТЗ

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Стальченко О.В.

Виконавець: ст. гр. ТКС-18м

Бакіссі Едена Маурісіна Бонже

Вінниця-2019

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “02” 10 2019 року № 254 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 02.09.2019 р.

Дата закінчення: 09.12.2019 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної магістерської кваліфікаційної роботи є підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії і скорочення часу встановлення захищеного з'єднання.

Задачами магістерської кваліфікаційної роботи є:

- розробка технічного завдання;
- дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості;
- розробка моделі порушника для оцінки захищеності системи IP-телефонії;
- розробка методики оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії;
- розробка пропозицій щодо модифікації протоколу розподілу ключів для поліпшення ймовірнісно-часових характеристик протоколу;
- розробка методу виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана;
- розробка пропозицій щодо модифікації протоколу Zimmermann Real-time Transport Protocol (ZRTP) для забезпечення безпеки кореспондентів при взаємодії без сервера в топології клієнт-клієнт.

Об’єкт дослідження є захищена IP-телефонія.

Предмет дослідження є методи і протоколи забезпечення інформаційної безпеки IP-телефонії, а також ймовірнісно-часові характеристики цих протоколів.

Основними завданнями роботи є:

- техніко-економічне обґрунтування доцільності даної розробки;
- аналіз поточного стану справ в області захищеної IP-телефонії;
- математична модель активного несанкціонованого доступу для захищеної IP-телефонії;
- розробка пропозицій щодо вдосконалення протоколів розподілу ключів;
- розробка пропозицій щодо поліпшення ймовірнісно-часових характеристик протоколу ZRTP;
- аналіз економічної ефективності проведеної розробки;
- дослідження питань безпеки життєдіяльності.

Модель порушника може бути використана при розробці методик контролю захищених мереж електрозв'язку. Метод виявлення порушника дозволяє автоматично виявити втручання порушника протоколів в канал зв'язку між кореспондентами для протоколу ZRTP без участі користувача.

Метод дозволяє знизити ймовірність успішної атаки НСД для порушника протоколів і може бути використаний при проектуванні, розробці та реалізації рішень захищеної IP-телефонії, що мають режим роботи без сервера, а також для удосконалення існуючих рішень.

Методика може бути використана для оцінки ефективності протоколів розподілу ключів, в частини часу виконання і ймовірності успішного завершення.

Методика оцінки ймовірнісно-часових характеристик може застосовуватися в розрахунках при проектуванні рішень по захищеної IP-телефонії, що використовують в своєму складі протоколи розподілу ключів.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на результатах звіту з переддипломної практики “Підвищення інформаційної безпеки IP-телефонії”, який виконувався у ВНТУ 2019/2020 н.р. Під час підготовки магістерської кваліфікаційної роботи будуть використані матеріали цього звіту.

Список використаних джерел розробки:

3.1 Скляр Б. Цифровая связь. Теоретические основы и применение / Бернард Скляр ; [пер. с англ]. – М.: Изд. Дом “Вильямс”, 2003. – 1104с.

3.2 Бахметьев, Б. Безопасность VoIP-соединений / Бахметьев Б. // Первая миля. - 2014. - № 2 (41). - С. 88-93.

3.3 Глотов, В. Правовые вопросы рынка VoIP / Глотов В. // Первая миля. - 2014. - № 2 (41). - С. 118-120.

3.4 Григорьев, В. А. Анализ пропускной способности сети радиосвязи стандарта IEEE 1609 / Григорьев В.А., Никитин В.Н., Кузнецов В.И., Тараканов С.А., Ковцур М.М. //Электросвязь.–2014– №.1.–с. 10-12

3.5 Никитин, В.Н. Обеспечение информационной безопасности ИТС / Никитин В.Н., Лагутенко О.И., Ковцур М.М. //Электросвязь.–2014– №.1. – с. 29-31

3.6 Ковцур М.М. Исследование путей совершенствования протоколов распределения ключей в защищенной IP-телефонии / М.М. Ковцур // Фундаментальные исследования. – 2014 – № 8(часть 6). – С. 1300-1308.

3.7 Коржик, В.И. Основы криптографии / В.И. Коржик, В.П. Просихин, В.А.Яковлев - СПб.: СПбГУТ, 2014. - 276 с.

3.8 Ковцур, М.М. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи / М. М. Ковцур, В.Н. Никитин, Д. В. Юркин // Информационно–управляющие системы. – 2014. – №1(68) – С. 70-75.

3.9 Ковцур, М.М. Оптимизация вероятностно-временных характеристик криптографического протокола распределения ключей IP-телефонии / М.М. Ковцур // Universum: технические науки. – 2014. – № 2 (3). – С. 1-9.

3.10 Положення про кваліфікаційну роботу у Вінницькому національному технічному університеті / Уклад. О. Н. Романюк, Р. Р. Обертюх, Т. О. Савчук, Л. П. Громова – Вінниця : ВНТУ, 2015 – 27 с.

3.11 Кухарчук В.В., Ігнатенко О.Г., Обертюх Р.Р. Методичні вказівки до оформлення дипломних проектів (робіт) для студентів всіх спеціальностей.- В.: ВДТУ, 2002.

3.12 Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – В.: ВДТУ, 2003.

3.13 ДСТУ 3008-2015. Інформація та документація, звіти у сфері науки і техніки.- К.: ДП «УкрНДНЦ», 2016.

3.14 Разработка и оформление конструкторской документации радиоэлектронной аппаратуры. Справочник. Под ред. Э.Т.Романычевой.- М: Радио и связь, 1989.

3.15 Бортник Г.Г., Васильківський М.В. Методичні вказівки до підготовки магістерських кваліфікаційних робіт для студентів спеціальності «Телекомунікації та радіотехніка» усіх форм навчання.- Вінниця:ВНТУ, 2018.- 50 с.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТКС-18м Бакіссі Едена Маурісіна Бонже

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження методу підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії і скорочення часу встановлення захищеного з'єднання.

Технічні вимоги, яким повинна відповідати розробка, наступні:

- клас якості обслуговування - 0;
- затримка доставки пакета IP, IPTD – 100 мс;
- варіація затримки пакета IP, IPDV (джиттер) – 50 мс;
- коефіцієнт втрати пакетів IP, IPLR - 10^{-3};
- коефіцієнт помилок пакетів IP, IPER - 10^{-4};
- протокол захисту при встановленні з’єднання - SIPS / TLS;
- протокол захисту при передаванні медіа-трафіку – SRTP;
- протокол захисту при розділенні ключів - ZRTP, SDES;
- метод підтримки VPN – PPTP.

При підвищенні рівня захищеності інформації в сеансах безпечної IP-телефонії і скороченні часу встановлення захищеного з'єднання слід максимально використовувати стандартні та уніфіковані телекомунікаційні засоби.

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документ-тація
		початок	закінчення		
1.	Розробка технічного завдання (ТЗ)	02.09.2019р.	06.09.2019р.	Розроблене ТЗ	Додаток А
2.	Аналіз поточного стану справ в області захищеної IP-телефонії	09.09.2019р.	13.09.2019р.	Проведений аналіз	Вступ. Розділ 1.

3.	Математична модель активного несанкціонованого доступу для захищеної IP-телефонії	16.09.2019р.	04.10.2019р.	Розроблена математична модель	Розділ 2
4.	Розробка пропозицій щодо вдосконалення протоколів розподілу ключів	07.10.2019р	25.10.2019р.	Розроблений метод розподілу ключів	Розділ 3
5.	Розробка пропозицій щодо поліпшення ймовірнісно-часових характеристик протоколу ZRTP	28.10.2019р.	08.11.2019р.	Характеристики і параметри	Розділ 4
6.	Аналіз економічної ефективності	11.11.2019р.	15.11.2019р.	Економічна частина МКР	Розділ 5
7.	Охорона праці та безпека в надзвичайних ситуаціях	18.11.2019р.	22.11.2019р.	Частина ОТ та БНС	Розділ 6
8.	Оформлення пояснювальної записки (ПЗ) та графічної частини	25.11.2019р.	29.11.2019р.	Оформлена документація	ПЗ та графічна частина
9.	Нормоконтроль, попередній захист, рецензування МКР	02.12. 2019р.	06.12.2019р.	Позитивні відзиви	Відзив. рецензія
10.	Захист МКР ЕК		09.12. 2019р.	Позитивний захист	Протокол ЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- принципова схема підключення оператора VoIP;
- архітектурна модель для підтримки QoS;
- структурна схема з'єднання в сценарії клієнт-клієнт;
- алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником;

- алгоритм дій при захопленні терміналу користувача зовнішнім порушником;

- алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником;

- алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником;

- економічна частина МКР;

- розділ ОП та БНС;

- рекомендації щодо подальшого використання розробленого методу підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії і скорочення часу встановлення захищеного з'єднання.

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій:

- Регіональний Центр експлуатації телекомунікаційної мережі України шляхом методу підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії;

- ПАТ "Укртелеком" шляхом впровадження нових методик скорочення часу встановлення захищеного з'єднання.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії і скорочення часу встановлення захищеного з'єднання.

8 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відзив і рецензія.

9 ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри.

Захист магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

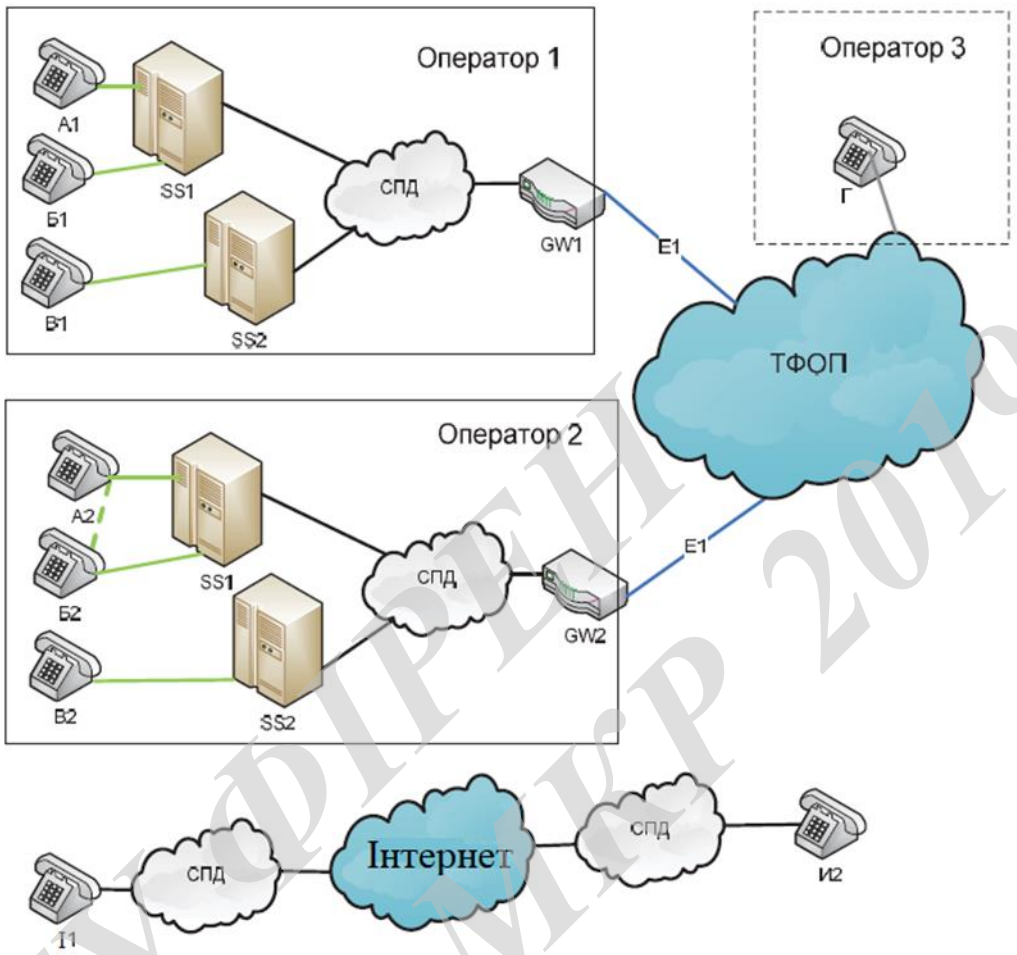
10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація, що розробляється в процесі виконання досліджень повинна містити:

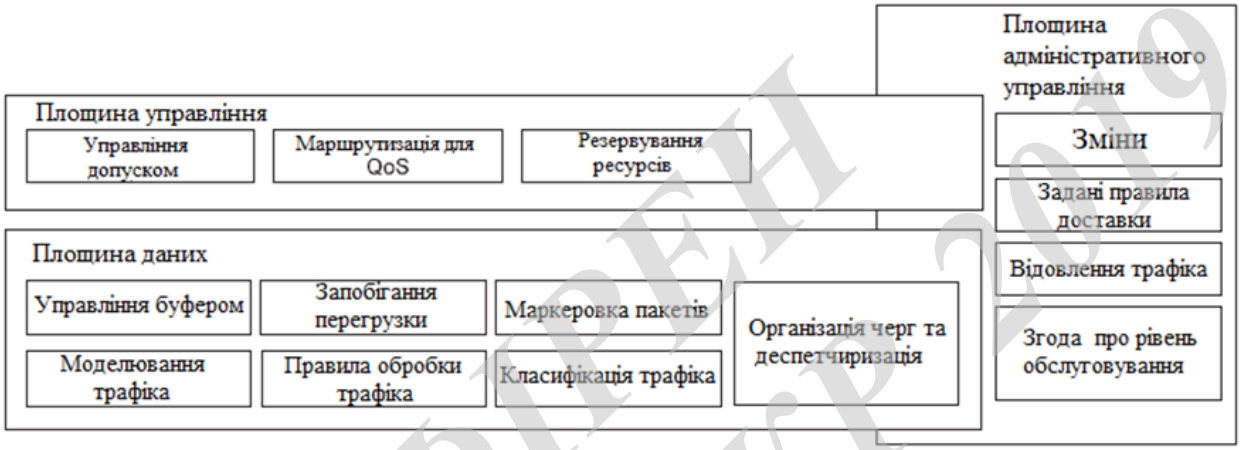
- техніко-економічне обґрунтування розробки;
- принципова схема підключення оператора VoIP;
- архітектурна модель для підтримки QoS;
- структурна схема з'єднання в сценарії клієнт-клієнт;
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії.

11 ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

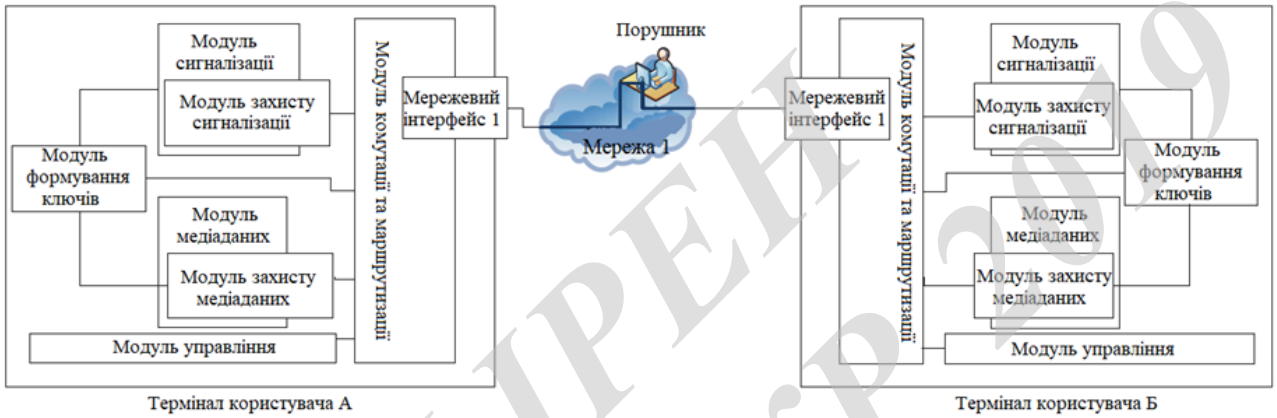
У зв’язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.



					08-34. МКР.001.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Бакіссі Едена			Принципова схема підключення оператора VoIP	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Стальченко О.В.					
Затверд.		Бортник Г.Г.					



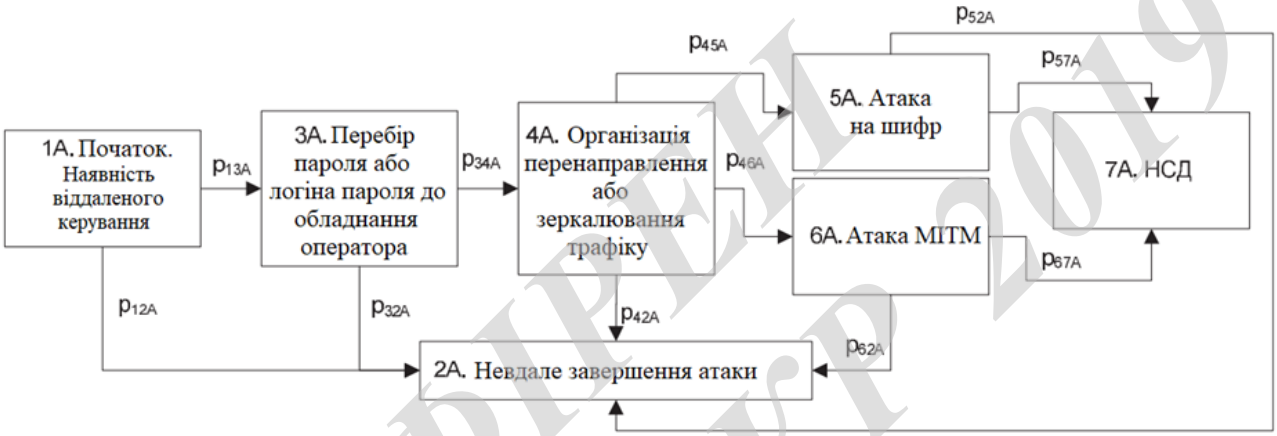
					08-34. МКР.001.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Бакіссі Едена			Архітектурна модель для підтримки QoS	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Стальченко О.В.					
Затверд.		Бортник Г.Г.					



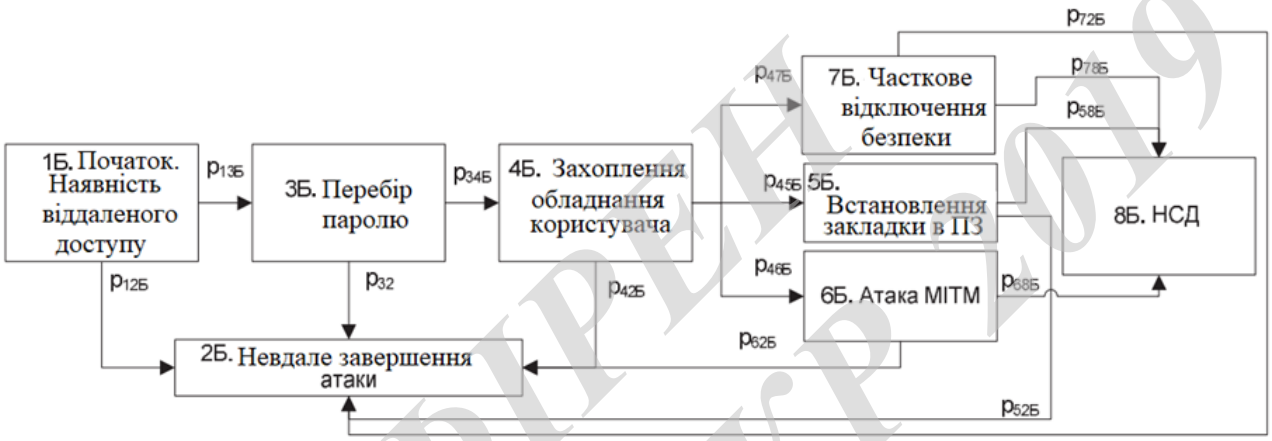
Термінал користувача А

Термінал користувача Б

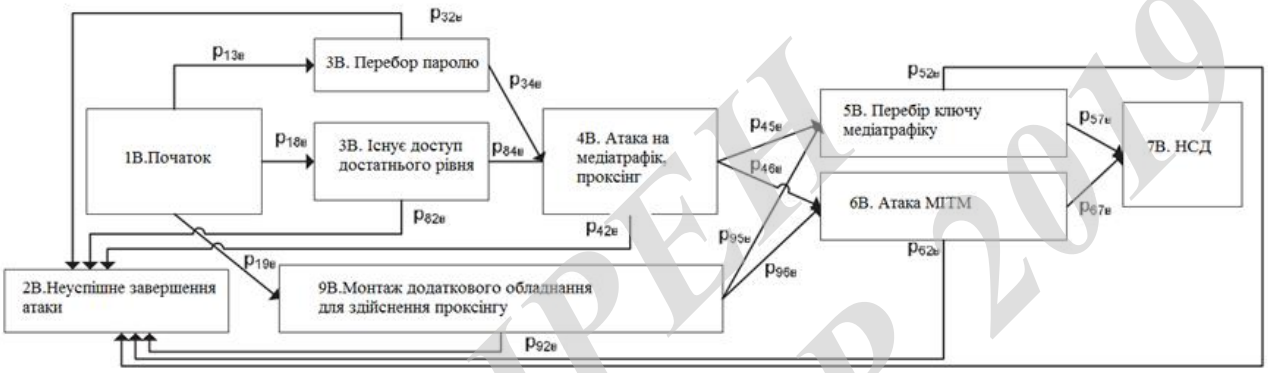
					08-34. МКР.001.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Бакіссі Едена			Структурна схема з'єднання в сценарії клієнт-клієнт	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Стальченко О.В.					
Затверд.		Бортник Г.Г.					



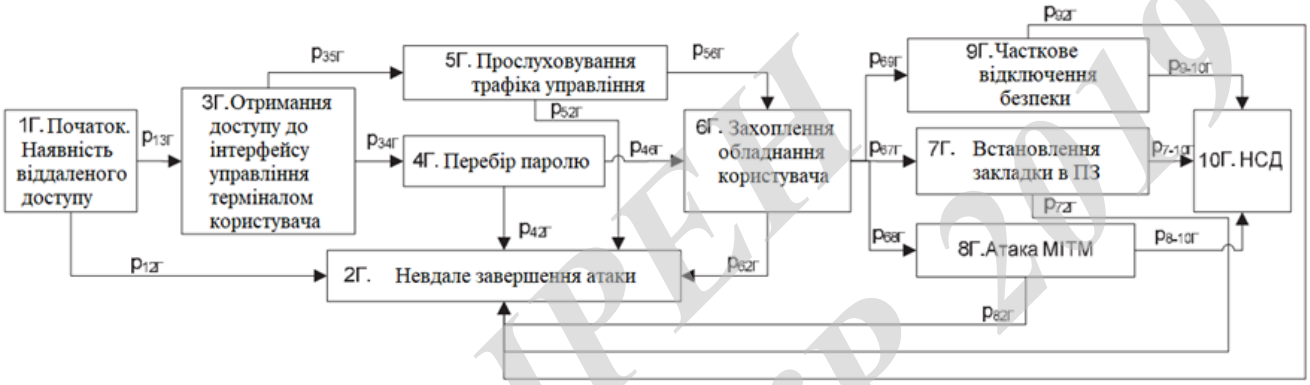
					08-34. МКР.001.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Бакіссі Едена			Алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Стальченко О.В.					
Затверд.		Бортник Г.Г.					



					08-34. МКР.001.00.000 Е8	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Бакіссі Едена			Алгоритм дій при захопленні терміналу користувача зовнішнім порушником	Літ. / Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.				
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м
Н. Контр.		Стальченко О.В.				
Затверд.		Бортник Г.Г.				



					08-34. МКР.001.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Бакіссі Едена			Алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Стальченко О.В.					
Затверд.		Бортник Г.Г.					



					08-34. МКР.001.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Бакіссі Едена			Алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником	Літ.	Арк. 1 / Аркушів 1
Перевір.		Стальченко О.В.					
Реценз.		Злепко С.М.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Стальченко О.В.					
Затверд.		Бортник Г.Г.					